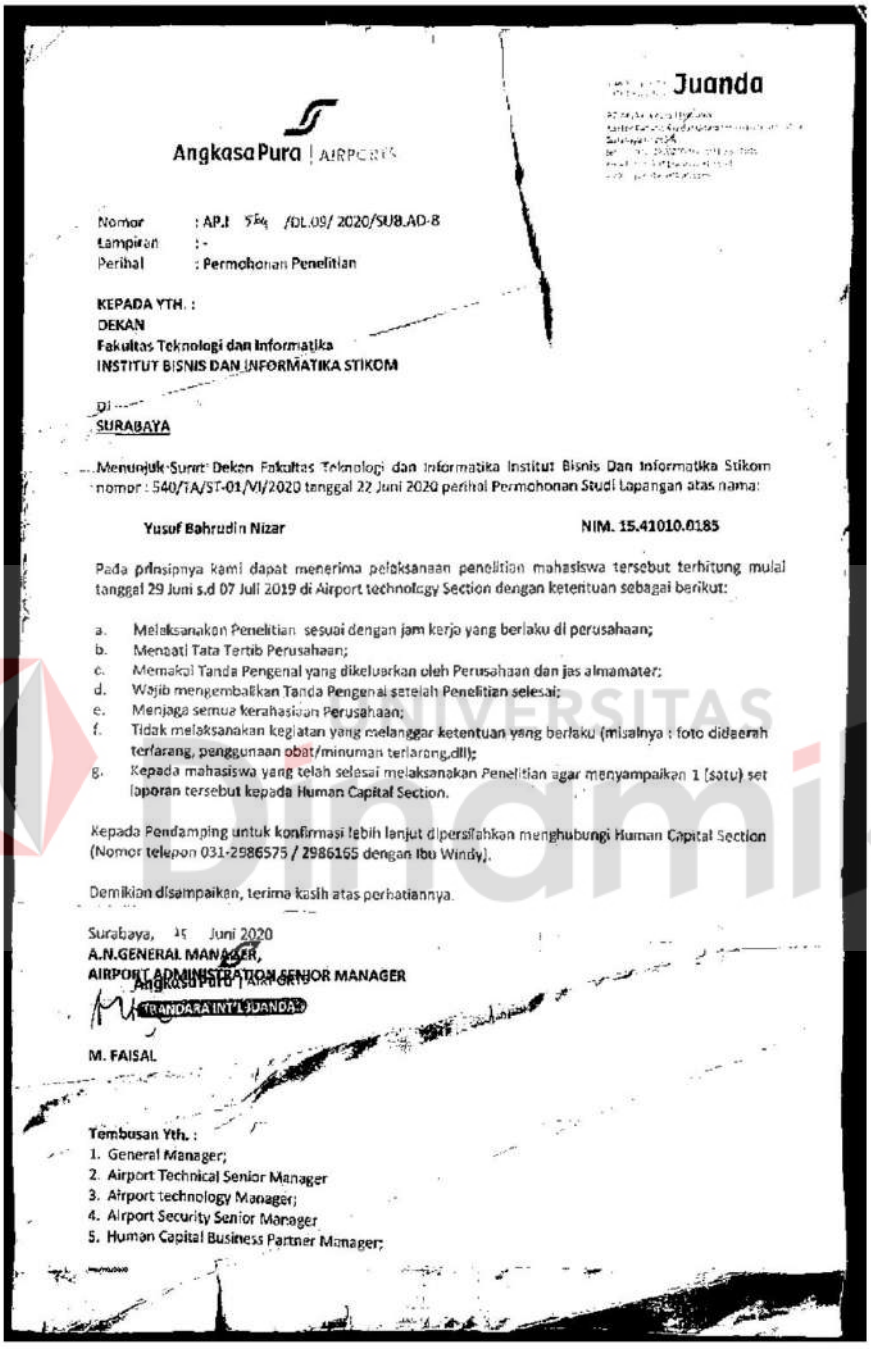
LAMPIRAN

1 SURAT IZIN INSTANSI



Juanda

Angkasa Pura | AIRPORTS

Nomor : AP.I 524 /DL.09/ 2020/SUB.AD-8
Lampiran : -
Perihal : Permohonan Penelitian

KEPADA YTH. :
DEKAN
Fakultas Teknologi dan Informatika
INSTITUT BISNIS DAN INFORMATIKA STIKOM

Di ---
SURABAYA

Menunjuk Surat Dekan Fakultas Teknologi dan Informatika Institut Bisnis Dan Informatika Stikom nomor : 540/TA/ST-01/VI/2020 tanggal 22 Juni 2020 perihal Permohonan Studi Lapangan atas nama:

Yusuf Bahrudin Nizar NIM. 15.41010.0185

Pada prinsipnya kami dapat menerima pelaksanaan penelitian mahasiswa tersebut terhitung mulai tanggal 29 Juni s.d 07 Juli 2019 di Airport technology Section dengan ketentuan sebagai berikut:

a. Melaksanakan Penelitian sesuai dengan jam kerja yang berlaku di perusahaan;
b. Mentaati Tata Tertib Perusahaan;
c. Memakai Tanda Pengenal yang dikeluarkan oleh Perusahaan dan jas almamater;
d. Wajib mengembalikan Tanda Pengenal setelah Penelitian selesai;
e. Menjaga semua kerahasiaan Perusahaan;
f. Tidak melaksanakan kegiatan yang melanggar ketentuan yang berlaku (misalnya : foto didaerah terlarang, penggunaan obat/minuman terlarang,dll);
g. Kepada mahasiswa yang telah selesai melaksanakan Penelitian agar menyampaikan 1 (satu) set laporan tersebut kepada Human Capital Section.

Kepada Pendamping untuk konfirmasi lebih lanjut dipersilahkan menghubungi Human Capital Section (Nomor telepon 031-2986575 / 2986165 dengan Ibu Windy).

Demikian disampaikan, terima kasih atas perhatiannya.

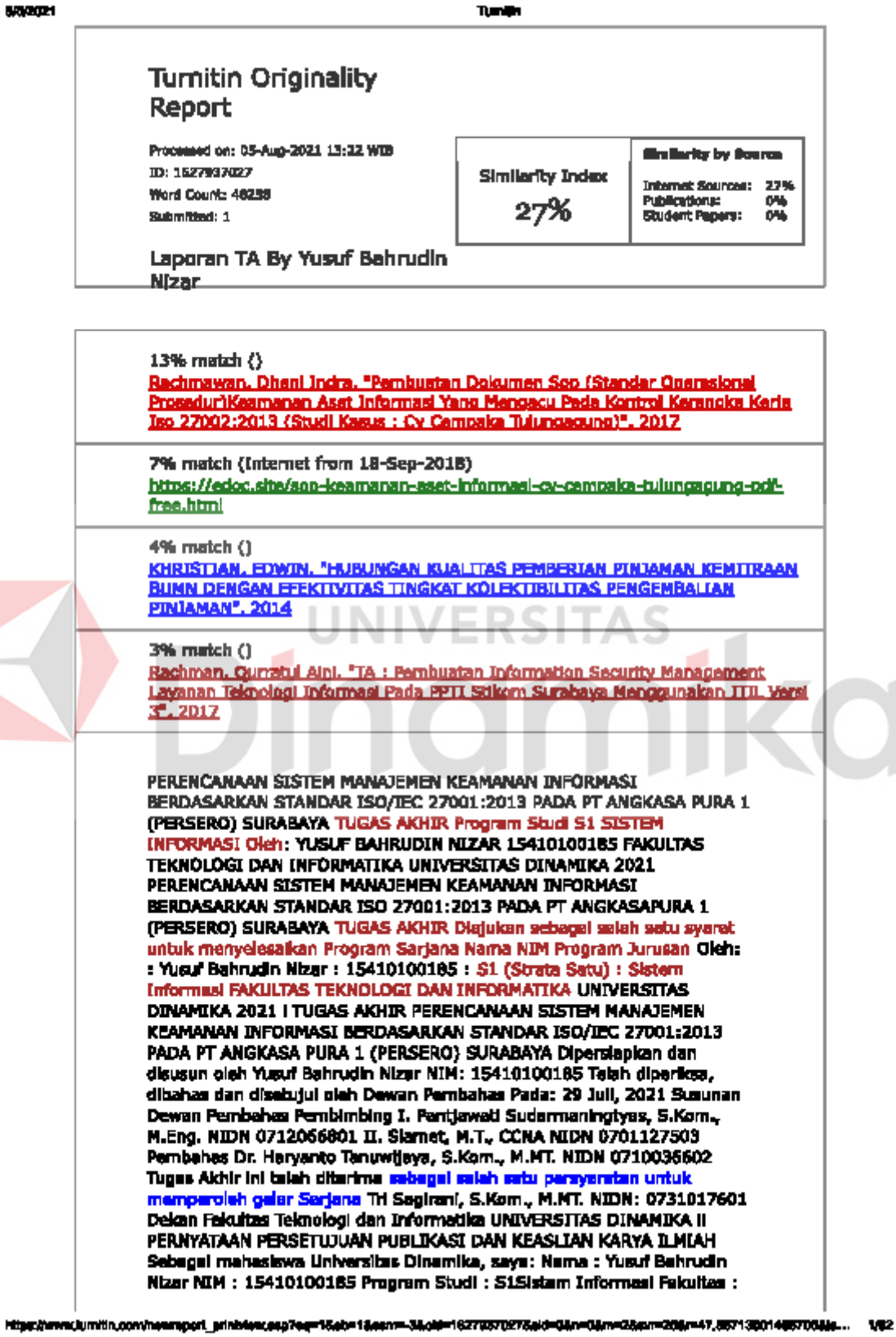
Surabaya, 15 Juni 2020
A.N.GENERAL MANAGER,
AIRPORT ADMINISTRATION SENIOR MANAGER

Angkasa Pura | AIRPORTS
TRANDARA INT'L JUANDA

M. FAISAL

Tembusan Yth. :
1. General Manager;
2. Airport Technical Senior Manager
3. Airport technology Manager;
4. Airport Security Senior Manager
5. Human Capital Business Partner Manager;

Bukti Originalitas Karya



5/5/2021 Turnitin

Turnitin Originality Report

Processed on: 05-Aug-2021 13:12 WIB
ID: 1627937027
Word Count: 46258
Submitted: 1

Laporan TA By Yusuf Bahrudin Nizar

Similarity Index	Similarity by Source
27%	Internet Sources: 23% Publications: 0% Student Papers: 0%

13% match ()
Rachmawan, Dhani Indra. "Pembuatan Dokumen Sop (Standar Oparasional Prosedur)Keamanan Aset Informasi Yang Mengacu Pada Kontrol Kerangka Kerja Iso 27002:2013 (Studi Kasus : Cv Cempaka Tulungagung)", 2017

7% match (Internet from 18-Sep-2018)
https://edoc.site/sop-keamanan-aset-informasi-cv-cempaka-tulungagung-pdf-free.html

4% match ()
KHRISTIAN, EDWIN. "HUBUNGAN KUALITAS PEMBERIAN PINJAMAN KEMITRAAN BUMN DENGAN EFEKTIVITAS TINGKAT KOLEKTIBILITAS PENGEMBALIAN PINJAMAN", 2014

3% match ()
Rachman, Qurratul Aini. "TA : Pembuatan Information Security Management Layanan Teknologi Informasi Pada PPTI Stikom Surabaya Menggunakan ITIL Versi 3", 2017

PERENCANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 PADA PT ANGKASA PURA 1 (PERSERO) SURABAYA TUGAS AKHIR Program Studi S1 SISTEM INFORMASI Oleh: YUSUF BAHRUDIN NIZAR 15410100185 FAKULTAS TEKNOLOGI DAN INFORMATIKA UNIVERSITAS DINAMIKA 2021 PERENCANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERDASARKAN STANDAR ISO 27001:2013 PADA PT ANGKASAPURA 1 (PERSERO) SURABAYA TUGAS AKHIR Diajukan sebagai salah satu syarat untuk menyelesaikan Program Sarjana Nama NIM Program Jurusan Oleh: : Yusuf Bahrudin Nizar : 15410100185 : S1 (Strata Satu) : Sistem Informasi FAKULTAS TEKNOLOGI DAN INFORMATIKA UNIVERSITAS DINAMIKA 2021 I TUGAS AKHIR PERENCANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 PADA PT ANGKASA PURA 1 (PERSERO) SURABAYA Dipersiapkan dan disusun oleh Yusuf Bahrudin Nizar NIM: 15410100185 Telah diperiksa, dibahas dan disetujui oleh Dewan Pembahas Pada: 29 Juli, 2021 Susunan Dewan Pembahas Pembimbing I. Pantjawati Sudarmaningtyas, S.Kom., M.Eng. NIDN 0712066801 II. Slamet, M.T., CCNA NIDN 0701127503 Pembahas Dr. Haryanto Tanuwijaya, S.Kom., M.MT. NIDN 0710036602 Tugas Akhir ini telah diterima sebagai salah satu persyaratan untuk memperoleh gelar Sarjana TI Sagirani, S.Kom., M.MT. NIDN: 0731017601 Dekan Fakultas Teknologi dan Informatika UNIVERSITAS DINAMIKA II PERNYATAAN PERSETUJUAN PUBLIKASI DAN KEASLIAN KARYA ILMIAH Sebagai mahasiswa Universitas Dinamika, saya: Nama : Yusuf Bahrudin Nizar NIM : 15410100185 Program Studi : S1Sistem Informasi Fakultas :

https://www.turnitin.com/newreport_printview.asp?eq=1&eb=1&esm=-3&oid=1627937027&sid=0&n=0&m=2&svr=208&r=47.85713801468570&lo... 1/62

LAMPIRAN 2

HASIL WAWANCARA

Lampiran 2.1 – Tujuan wawancara

Wawancara ke-	Narasumber	Jabatan	Tujuan Wawancara
1	Bapak Didik Hermanto	*ICT Department Head*	Penggalian informasi mengenai visi, misi tujuan instansi, tugas, fungsi dan struktur organisasi, serta proses bisnis PT Angkasa Pura 1 Surabaya, fungsi-fungsi yang ada di dalamnya
2	Bapak Sukirman	*Airport Security Department Head*	Penggalian informasi mengenai pengelolaan asset sistem informasi, teknis mengenai penggunaan hardware, software, *database* dan jaringan, kelemahan teknologi informasi, risiko keamanan yang pernah terjadi dan laporan rekapitulasi keamanan informasi.

Lampiran 2.2 – Detail Ringkas Pertanyaan

No.	Detail Ringkas Pertanyaan	Tujuan Wawancara
1	Penggalian informasi mengenai visi, misi Tujuan instansi, tugas, fungsi, dan struktur organisasi, serta proses bisnis PT Angkasa Pura 1 Surabaya, informasi pengelolaan asset sistem informasi, teknis mengenai penggunaan *hardware, software, database* dan jaringan, kelemahan teknologi informasi, risiko keamanan yang pernah terjadi dan laporan rekapitulasi keamanan informasi	- Data Visi, Misi, dan tujuan instansi - Data Tugas, Fungsi dan Struktur Organisasi instansi - Proses bisnis PT Angkasa Pura 1 Surabaya - Penggunaan IT dalam Operasional Bisnis - Praktik Pengamanan yang telah dilakukan - Identifikasi Risiko Keamanan aset Informasi - Risiko yang terjadi beserta penyebab dan dampaknya

Lampiran 1.3 – Daftar Hasil Wawancara

Nama Nara Sumber : Bapak Didik Hermanto Tanggal : -

Jabatan : ICT Department Head Waktu : 10.00 WIB

	Pertanyaan	Jawaban
1.	Informasi Narasumber	
	Apakah Peran dan Tanggung Jawab anda Sebagai Kepala bagian ICT?	Mempunyai tugas melaksanakan Sebagian tugas di bidang teknologi dan Informasi, yakni meliputi Menyusun dan melaksanakan rencana program dan petunjuk teknis, melaksanakan koordinasi dan kerjasama dengan bagian *Airport Security Department Head,* ATNOS, dan AOS, melaksanakan pengawasan dan pengendalian, melaksanakan evaluasi dan pelaporan, dan melaksanakan tugas-tugas lain yang diberikan oleh Manajer sesuai dengan tugas dan fungsinya.
	Apa sajakah aktivitas dan fungsi TI dalam proses bisnis PT Angkasa Pura 1 Surabaya?	Untuk proses bisnis berkaitan dengan fungsi TI yaitu layanan *Flight Information Display System* (FIDS), Aplikasi Counter *check-in*, monitoring rutin keamanan server hosting untuk proses keamanan informasi. Serta juga ada aplikasi internal perusahaan seperti *E-Procurement Planning, E-IT Quality Planning, E-Maintenance Facilities*
2.	Keamanan Aset Informasi	
	Menurut anda, apa sajakah data dan asset yang kritikal atau paling penting dalam operasional di PT Angkasa Pura 1 Surabaya?	Semua data pada instansi ini menurut saya semua penting. tetapi data yang paling penting yaitu data *center* sebagai data pusat, data penerbangan, data maskapai, keuangan, dan data aset informasi pada instansi.
	Siapa sajakah yang memiliki hak akses terhadap asset informasi kritikal tersebut?	Untuk pemilik hak akses terhadap asset informasi pada instansi yaitu jajaran tinggi, seluruh kepala bidang, kepala staff dan Sebagian pegawai yang kami berikan hak akses sebagai pengguna aplikasi.

Lampiran 1.4 – Daftar Hasil Wawancara 2

Nama Narasumber : Sukirman Tanggal : -

Jabatan : *Airport Security Department Head* Waktu : 10.10 WIB

No.	Pertanyaan	Jawaban
1.	Pengelolaan asset informasi	
	1. Apakah PT Angkasa Pura telah memiliki Prosedur dalam pencegahan terhadap kerusakan pada asset informasi yang dimiliki saat ini?	Sudah ada namun belum terlaksanakan dengan baik. Masih ada yang belum terdokumentasi dengan baik.
2.	Identifikasi Ancaman serta cara pengamanan	
	1. Apakah dampak dari masing2 ancaman (Yang disebutkan sebelumnya) tersebut terhadap berjalannya proses bisnis?	Jawaban ada pada lampiran 4 tentang daftar kejadian yang pernah terjadi pada instansi
	2. Apa sajakah ancaman yang pernah terjadi terhadap asset informasi kritikal tersebut?	
	3. Apa saja praktek pengamanan yang telah dilakukan oleh PT Angkasa Pura 1 Surabaya terhadap aset informasi kritikal tersebut?	

Visi, Misi dan Tujuan

Visi

Menjadi pengelola dan penyedia jasa teknologi informasi dan komunikasi internal berstandar internasional

Misi

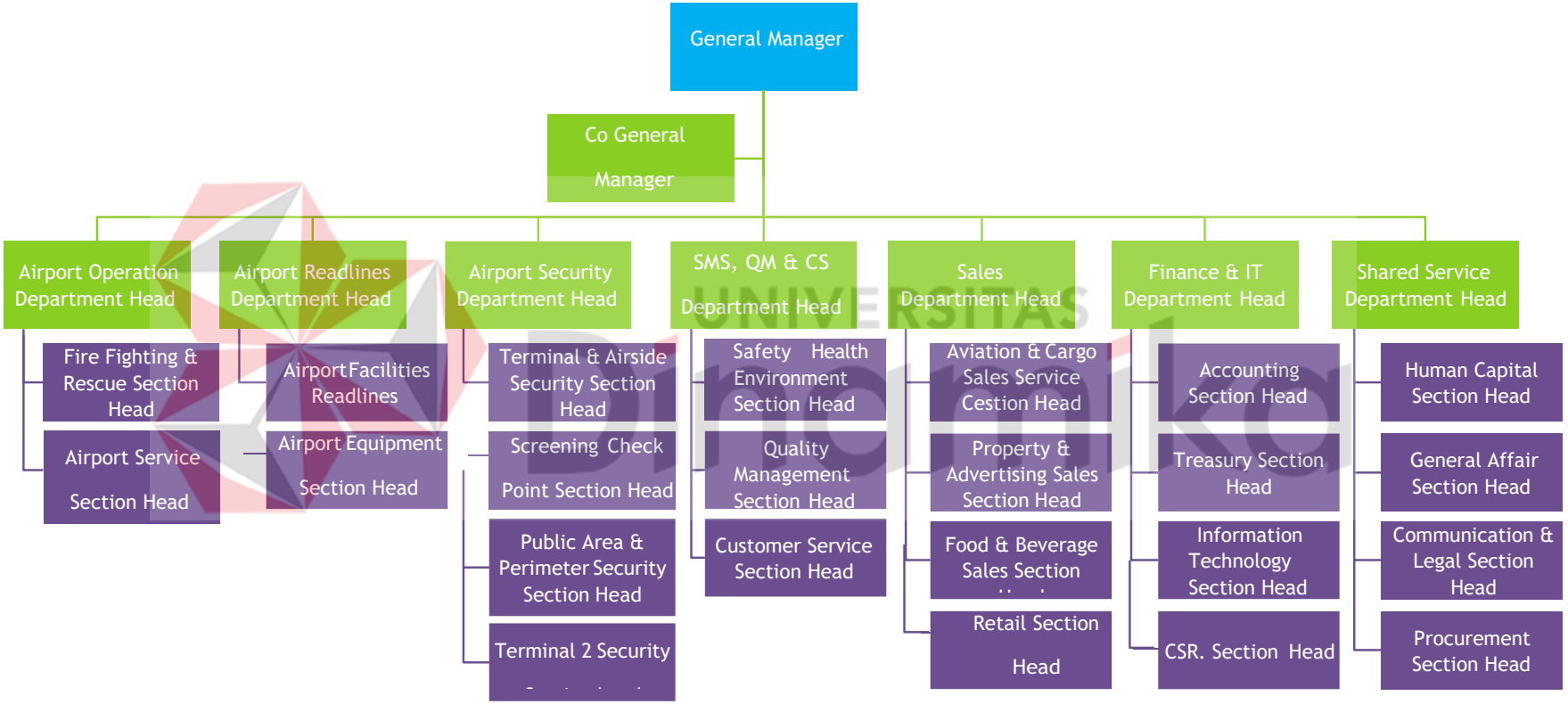
Menyediakan layanan teknologi informasi dan komunikasi yang prima dan tepat kepada *stakeholder* dengan tujuan:

1. Meningkatkan nilai dan daya saing perusahaan
2. Meningkatkan kinerja perusahaan
3. Meningkatkan kemampuan pelayanan perusahaan.
4. Menciptakan jasa nilai tambah

Tujuan

1. Melaksanakan dan menunjang kebijakan program pemerintah di bidang ekonomi dan pembangunan
2. Menghasilkan keuntungan bagi perseroan dengan menyelenggarakan usaha jasa kebandarudaraan
3. Menghasilkan keuntungan bagi usaha-usaha lainnya yang mempunyai hubungan dengan usaha perusahan

Struktur Organisasi



LAMPIRAN 3

TUGAS POKOK DAN FUNGSI

1. GENERAL MANAGER

Tanggung jawab *General Manager* dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1) adalah sebagai berikut:

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan perannya sebagai *people manager* pada unit kerjanya;
d. Memastikan kegiatan di Bandar Udara berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan di Bandar Udara sesuai dan relevan dengan sistem manajemen yang diterapkan perusahaan;
f. Memastikan tercapainya *Customer Satisfaction Index* (CSI);
g. Memastikan tercapainya pendapatan *non* aeronautika;
h. Memastikan kontribusi terhadap lingkungan.

2. CO. GENERAL MANAGER

Tanggung jawab Co. General Manager dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1) adalah sebagai berikut:

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan perannya sebagai *people manager* pada unit kerjanya;
d. Memastikan kegiatan di Bandar Udara berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan di Bandarudara sesuai dan relevan dengan sistem manajemen yang diterapkan perusahaan;
f. Memastikan tercapainya *Customer Satisfaction Index* (CSI);
g. Memastikan kualitas laporan, dan konsep dari setiap *Department Head* melalui pemeriksaan, perbaikan, evaluasi dan pengelolaan administrasi baik secara offline maupun *online* secara efektif.

3. AIRPORT OPERATION AND SERVICES DEPARTMENT HEAD

Tanggung jawab *Airport Operation and Services Department Head* dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1) adalah sebagai berikut:

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan perannya sebagai *people manager* pada unit kerjanya;

d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan perusahaan;
f. Memastikan pelaksanaan kegiatan *customer service*, *airport hospitality*, *airport operational support*, *airport rescue* dan *firefighting* berdasarkan kebijakan dan strategi sumber daya manusia, fasilitas, pedoman serta Standar Operasional Prosedur (SOP).

4. CUSTOMER SERVICE AND HOSPITALITY SECTION HEAD

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan perannya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan perusahaan;
f. Memastikan pengelolaan komplain pelanggan telah ditindaklanjuti;
g. Memastikan pelaksanaan kegiatan *customer service* dan *airport hospitality* berdasarkan kebijakan, strategi dan Standar Operasional Prosedur (SOP).

5. Airport Operation Air Side Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan perannya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan perusahaan;
f. Memastikan kesiapan fasilitas dalam mendukung kegiatan operasional bidang sisi udara (air side) dan sumber daya manusia berdasarkan kebijakan, strategi dan Standar Operasional Prosedur (SOP).

6. Airport Operation Landside and Terminal Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;

e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan perusahaan;
f. Memastikan kesiapan fasilitas dalam mendukung kegiatan operasional bidang sisi darat (*land side*) dan terminal serta sumber daya manusia berdasarkan kebijakan, strategi dan Standar Operasional Prosedur (SOP).

7. Airport Rescue and Fire Fighting Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan perusahaan;
f. Memastikan kesiapan fasilitas dan serta sumber daya manusia bidang *airport rescue* and *fire fighting* di bandar udara berdasarkan kebijakan, strategi dan Standar Operasional Prosedur (SOP).

8. AIRPORT SECURITY DEPARTMENT HEAD

Tanggung jawab Airport Security Department Head dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1) adalah sebagai berikut:
a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan perusahaan;
f. Memastikan pelaksanaan kegiatan *airport security screening, non-terminal protection security, dan terminal protection security* berdasarkan kebijakan dan strategi sumber daya manusia, fasilitas, pedoman serta Standar Operasional Prosedur (SOP);
g. Memastikan terlaksananya koordinasi keamanan dengan pihak eksternal;
h. Memastikan tercapainya level *of service* keamanan penerbangan;
i. Memastikan tersedia dan terimplementasinya *Airport Security Programme* (ASP) dan Standar Operasional Prosedur (SOP) yang telah ditetapkan dan dilaksananakan secara konsisten.

9. Airport Security Screening Selection Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan perusahaan;
f. Memastikan terlaksananya kegiatan *airport security screening* sesuai dengan *Airport Security Programme* (ASP) dan Standar Operasional Prosedur (SOP) yang telah ditetapkan dan dilaksanakan secara konsisten;
g. Memastikan tersedianya sumber daya manusia yang memiliki kompetensi *screening* dan tersedianya fasilitas serta Standar Operasional Prosedur (SOP) pemeriksaan keamanan penumpang, personel pesawat udara, orang perseorangan dan barang;
h. Memastikan *design* dan *layout airport security screening* sesuai dengan fungsi keamanan penerbangan.

10. Terminal Protection Security Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan perusahaan;
f. Memastikan terlaksananya kegiatan keamanan terminal sesuai dengan *Airport Security Programme* (ASP) dan Standar Operasional Prosedur (SOP) yang telah ditetapkan dan dilaksanakan secara konsisten;
g. Memastikan tersedianya fasilitas, sumber daya manusia dan Standar Operasional Prosedur (SOP) *terminal protection security;*
h. Memastikan *design* dan *layout* bandar udara sesuai dengan fungsi keamanan penerbangan.

11. Non-Terminal Protection Security Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;

f. Memastikan terlaksananya kegiatan keamanan non terminal sesuai dengan *Airport Security Programme* (ASP) dan Standar Operasional Prosedur (SOP) yang telah ditetapkan dan dilaksanakan secara konsisten;
g. Memastikan tersedianya kebijakan dan strategi sumber daya manusia, fasilitas dan Standar Operasional Prosedur (SOP) *non terminal protection security;*
h. Memastikan *design* dan *layout* bandar udara sesuai dengan fungsi keamanan penerbangan.

12. AIRPORT SAFETY & QUALITY MANAGEMENT DEPARTMENT HEAD

Tanggung jawab Airport Safety and Quality Management Department Head dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1) adalah sebagai berikut:

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yamg diterapkan Perusahaan;
f. Memastikan dilaksanakannya standar Keselamatan dan Kesehatan Kerja (K3) di perusahaan;
g. Memastikan tercapainya *safety level*, *quality manajemen* dan *risk management* di bandar udara sesuai dengan ketentuan yang telah ditetapkan.

13. Safety Management System and Occupational Safety Health Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan pencapaian *safety level* melalui mitigasi *hazard* guna mendukung tingkat kesehatan optimal di lingkungan Perusahaan;
g. Memastikan tidak terjadinya kecelakaan kerja dalam setiap pelaksanaan pekerjaan;

h. Memastikan setiap rekomendasi yang dihasilkan dapat diimplementasikan;
i. Memastikan setiap pelaksanaan pekerjaan bidang *safety management system* dan *occupational safety health* sesuai dengan kebijakan, strategi dan Standar Operasional Prosedur (SOP)

14. Risk Management Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan *risk management* sesuai dengan ketentuan yang telah diterapkan;
g. Memastikan tersedianya *risk profile* dan *mitigation plan.*

15. Airport Equipment Readiness Department Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan kepuasan pelanggan bandar udara sesuai dengan ketentuan yang berlaku;
g. Memastikan kesiapan operasional seluruh fasilitas peralatan (equipment) bandar udara;
h. Memastikan tercapainya tingkat *level of service* sesuai standar minimum ketentuan yang berlaku.

16. Mechanical Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;

d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan kesiapan layak operasional peralatan meliputi *mechanical*, *heavy equipment* dan *water technique* bagi pelayanan bandar udara;
g. Memastikan kenyamanan penggunaan jasa bandar udara.

17. Electrical Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan kesiapan layak operasional peralatan meliputi *electrical* bagi pelayanan bandar udara;
g. Memastikan kenyamanan pengguna jasa bandar udara.

18. Airport Facilities Readiness Department Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan tersedianya fasilitas bandar udara yaitu sisi udara (air side), sisi darat (land side), *landscape* dan *terminal building* yang siap digunakan;
g. Memastikan tersedianya pengelolaan *environment* bandar udara.

19. Non-Terminal Air Side Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;

e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan tersedianya fasilitas bandar udara khususnya sisi udara (*air side*) yang siap digunakan sesuai dengan kebijakan, strategi dan Standar Operasional Prosedur (SOP).

20. Non-Terminal Land Side, Landscape and Environmental Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan tersedianya fasilitas bandar udara khususnya non terminal sisi darat (*land side*) dan *landscape* yang handal dan siap digunakan sesuai dengan kebijakan, strategi dan Standar Operasional Prosedur (SOP).
g. Memastikan tersedianya dokumen lingkungan, Laporan Rencana Pengelolaan Lingkungan (RKL) dan Rencana Pemantauan Lingkungan (RPL) pada tiap semester berdasarkan ketentuan yang berlaku;
h. Memastikan tersedia dan terlaksananya dokumen *ecological airport* sesuai *ecological airport master plan.*

21. Terminal Building Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan tersedianya fasilitas bandar udara khususnya *terminal building* yang siap digunakan sesuai dengan kebijakan, strategi dan Standar Operasional Prosedur (SOP).

22. Sales Department Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;

d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan tercapainya *portofolio* pendapatan *aviation* dan *non-aviation;*
g. Memastikan tercapainya target efektivitas penyaluran dan kolektabilitas Program Kemitraan dan Bina Lingkungan.

23. Aviation and Cargo Sales Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan tercapainya *portofolio* pendapatan dari bisnis *aviation dan cargo.*

24. Property and Advertising Sales Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan tercapainya *portofolio* pendapatan dari penjualan bisnis *property* dan *advertising*.

25. Food and Beverage Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;

f. Memastikan tercapainya *portofolio* pendapatan dari bisnis *food and beverage sales.*
g. Memastikan terpenuhinya kepuasan *tenant* atas layanan bisnis *food and beverage sales.*

26. Retail Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan tercapainya *portofolio* pendapatan dari bisnis *retail.*
g. Memastikan terpenuhinya kepuasan *tenant* atas layanan bisnis *retail.*

27. Corporate Social Responsibility

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan penyampaian usulan jumlah calon mitra binaan;
g. Memastikan realisasi program penyaluran bina lingkungan yang telah disetujui;
h. Memastikan pelaksanaan survei. Penyaluran, penagihan, pemantauan (*monitoring)* dan pembinaan sesuai dengan usulan yang telah ditetapkan;
i. Memastikan pencatatan dan laporan akuntansi Program Kemitraan dan Bina Lingkungan (PKBL) diselesaikan tepat waktu dan sesuai standar akuntansi Program Kemitraan dan Bina Lingkungan (PKBL).

28. Information Communication Technology Department Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;

f. Memastikan layanan *Information Communication Technology* (ICT) *meliputi security equipment, airport communication, network, information communication technology business operation and support di bandar udara berfungsi dengan baik;*
g. *Memastikan perawatan (maintenance)* atas sistem *Information Communication Technology* (ICT) di bandar udara;
h. Memastikan terimplementasinya kebijakan, strategi, tata kelola dan Standar Operasional Prosedur (SOP) serta program korporat terkait *Information Communication Technology* (ICT) yang telah ditetapkan oleh kantor pusat.

29. Application Operation and Support Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan terlaksananya fungsi *Information Communication Technology* (ICT) di bidang *application operation* di bandar udara;
g. Memastikan tertanganinya semua keluhan dan permasalahan atas layanan operasional *Information Communication Technology* (ICT).

30. Airport Technology, Network Operation and Support Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan terlaksananya fungsi *Information Communication Technology* (ICT) di bidang *airport technology* dan *network operation* di bandar udara;
g. Memastikan tertanganinya semua keluhan dan permasalahan atas layanan jaringan dan infrastruktur *Information Communication Technology* (ICT).

31. Finance Department Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan ketepatan perencanaan kebutuhan dana Kantor Cabang;
g. Memastikan tercapainya target kolektabilitas piutang usaha;
h. Memastikan realisasi anggaran biaya dilaksanakan sesuai Rencana Kerja dan Anggaran Perusahaan (RKAP).

32. Accounting Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan tercapainya target waktu dan akurasi pelaporan;
g. Memastikan terpenuhinya syarat-syarat dokumen penerimaan dan pengeluaran kas/bank;

33. Treasury Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan operasional penerimaan dan pengeluaran kas/bank berjalan dengan lancar dan tidak terjadi kesalahan;
g. Memastikan perencanaan, perhitungan dan pelaporan pajak dilaksanakan dengan akurat dan tepat waktu.

a. Account Receivable Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan terlaksananya kegiatan konfirmasi, pemantauan, (*monitoring*) dan penagihan piutang sesuai dengan rencana yang ditetapkan;
g. Memastikan tertagihnya piutang tepat waktu;
h. Memastikan terealisasinya komitmen pembayaran piutang.

34. Shared Services Department Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan tercapainya kepuasan pelanggan atas *shared services.*

35. Human Capital Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan terimplementasikannya pengelolaan *human capital administration* dan *industrial relation* berdasarkan ketentuan yang berlaku.

36. General Affair Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;

d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan tersedianya pelayanan perkantoran dalam mendukung operasional Perusahaan;
g. Memastikan ketersediaan, kesiapan pakai dan pemeliharaan fasilitas kerja berdasarkan Rencana Kerja dan Anggaran Perusahaan (RKAP);
h. Memastikan terjaganya hubungan baik dengan pihak internal dan eksternal;
i. Memastikan kegiatan keprotokolan berjalan dengan baik;
j. Memastikan ketersediaan dan pemeliharaan kebersihan sisi udara (*air side*), sisi darat (*land side*), landscape, gedung terminal dan area perkantoran.

37. Asset Management Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Menyetujui *Distinct Job Profile* (DJP) di ruang lingkup unit kerjanya;
g. Menyetujui pengenaan sanksi kepada personil di unit kerjanya sesuai dengan ketentuan yang berlaku di perusahaan;
h. Menyetujui pelaksanaan rencana kerja di lingkup unit kerjanya;
i. Menetapkan dan/atau menandatangani dokumentasi sistem manajemen yang menjadi ruang lingkup unit kerjanya;
j. Menetapkan metode dalam penyediaan dan penyiapan fasilitas perkantoran dalam mendukung operasional Perusahaan;
k. Memiliki akses kepada pihak-pihak terkait guna mendukung kegiatan keprotokolan;
l. Mengawasi pelaksanaan pemeliharaan kebersihan sisi udara *(air side)*, sisi darat *(land slide)*, *landscape*, gedung terminal dan area perkantoran.

38. Communication and Legal Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;

e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan terjaganya hubungan baik dengan pihak internal dan eksternal;
g. Memastikan kelancaran informasi dan data yang valid kepada pihak internal maupun eksternal;
h. Memastikan terlaksananya pengelolaan tata usaha dan arsip dengan baik;
i. Memastikan tercapainya pengelolaan hukum dengan baik.

39. Airport Duty Manager

a. Memastikan perannya sebagai *people manager* pada unit kerjanya;
b. Memastikan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
c. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang ditetapkan Perusahaan;
d. Memastikan kesiapan dan kelancaran operasional bandar udara.

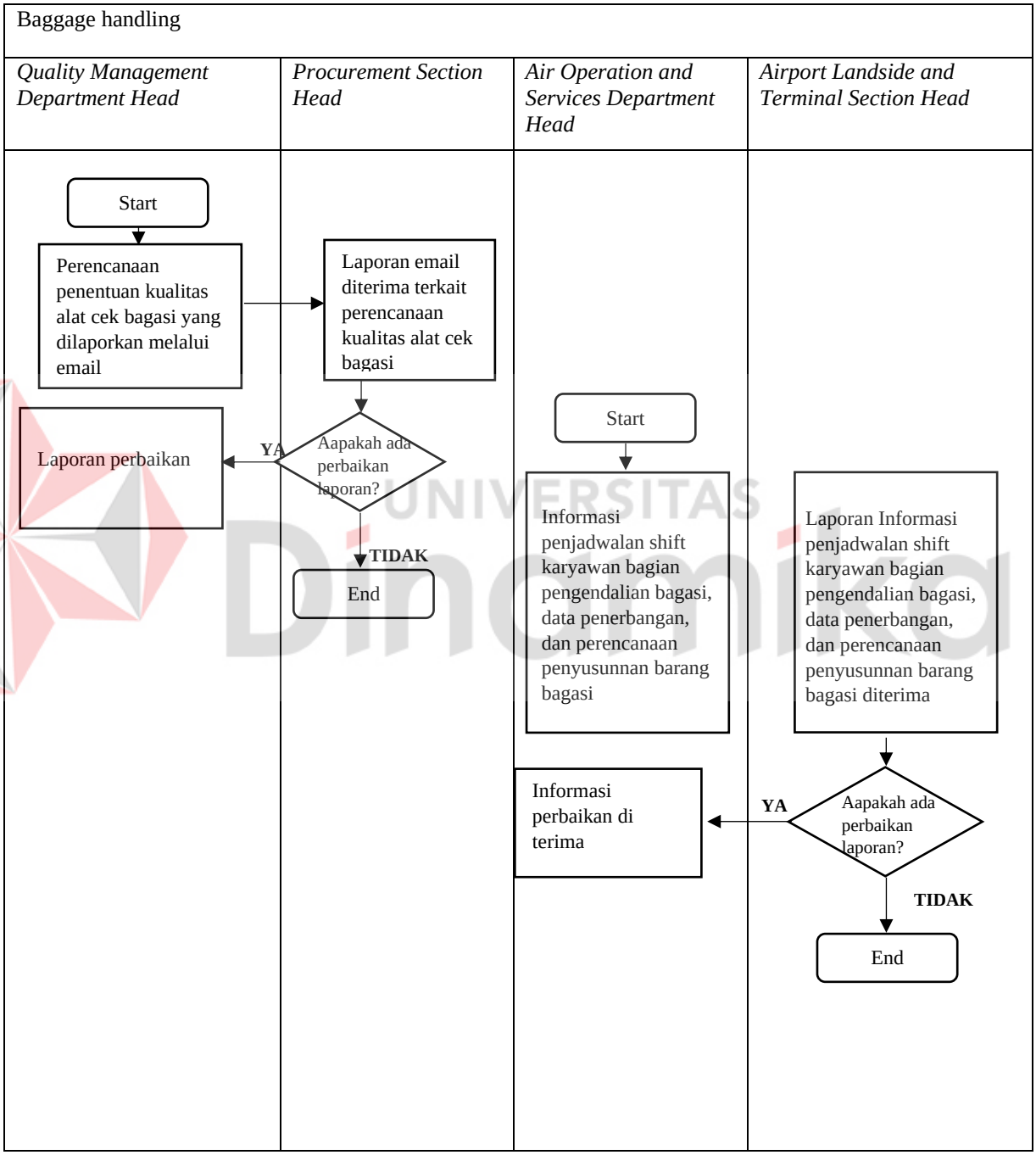
40. Procurement Section Head

a. Memastikan tersedianya Rencana Kerja dan Anggaran Perusahaan (RKAP)
b. Memastikan tercapainya kontrak manajemen yang telah disepakati;
c. Memastikan peranya sebagai *people manager* pada unit kerjanya;
d. Memastikan pelaksanaan kegiatan unit kerjanya berjalan sesuai dengan Rencana Kerja dan Anggaran (RKA) yang telah ditetapkan;
e. Memastikan pelaksanaan kegiatan unit kerjanya sesuai dan relevan dengan sistem manajemen yang diterapkan Perusahaan;
f. Memastikan pengadaan barang/jasa sesuai dengan pedoman yang berlaku.

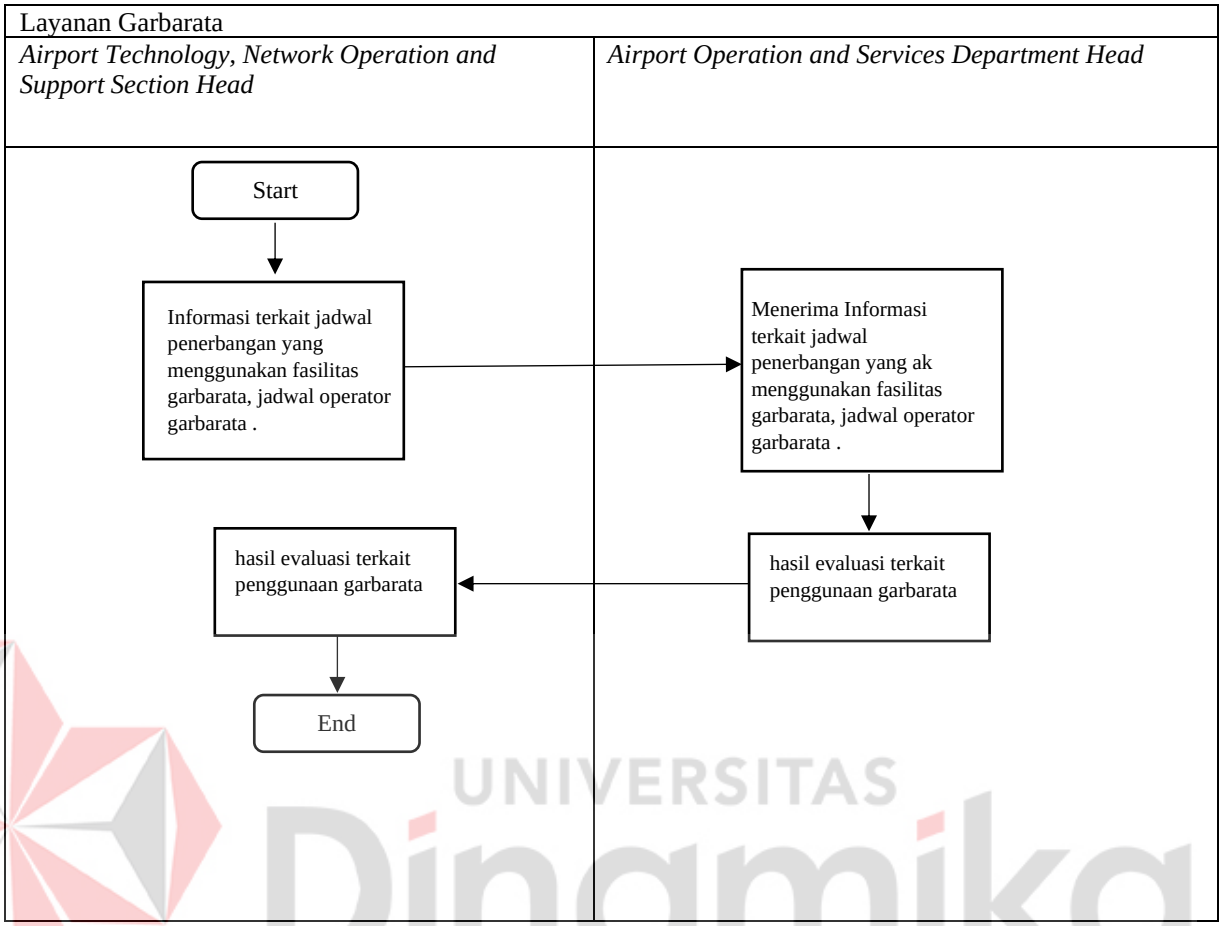
LAMPIRAN 4

DOKULMEN PROSES BISNIS

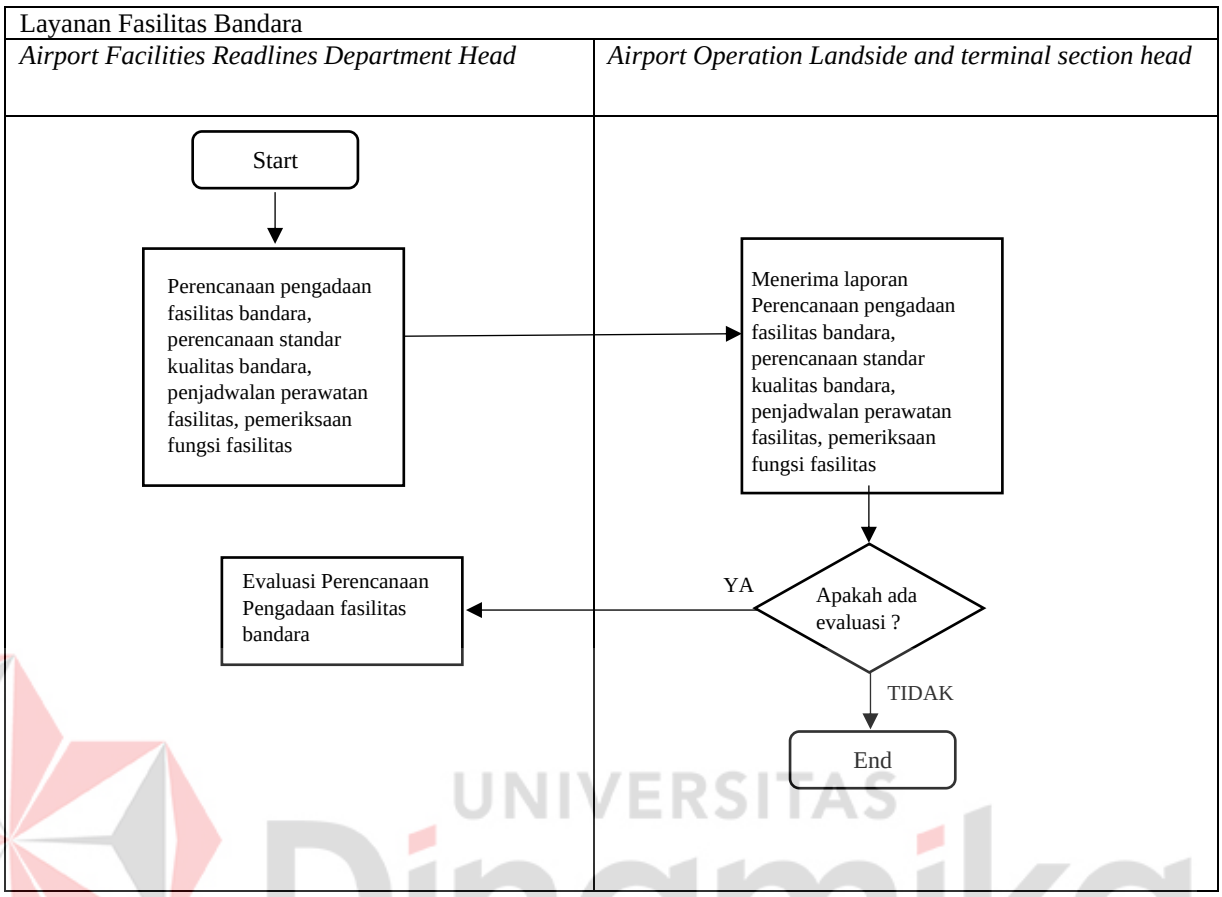
1) Pengendalian Bagasi

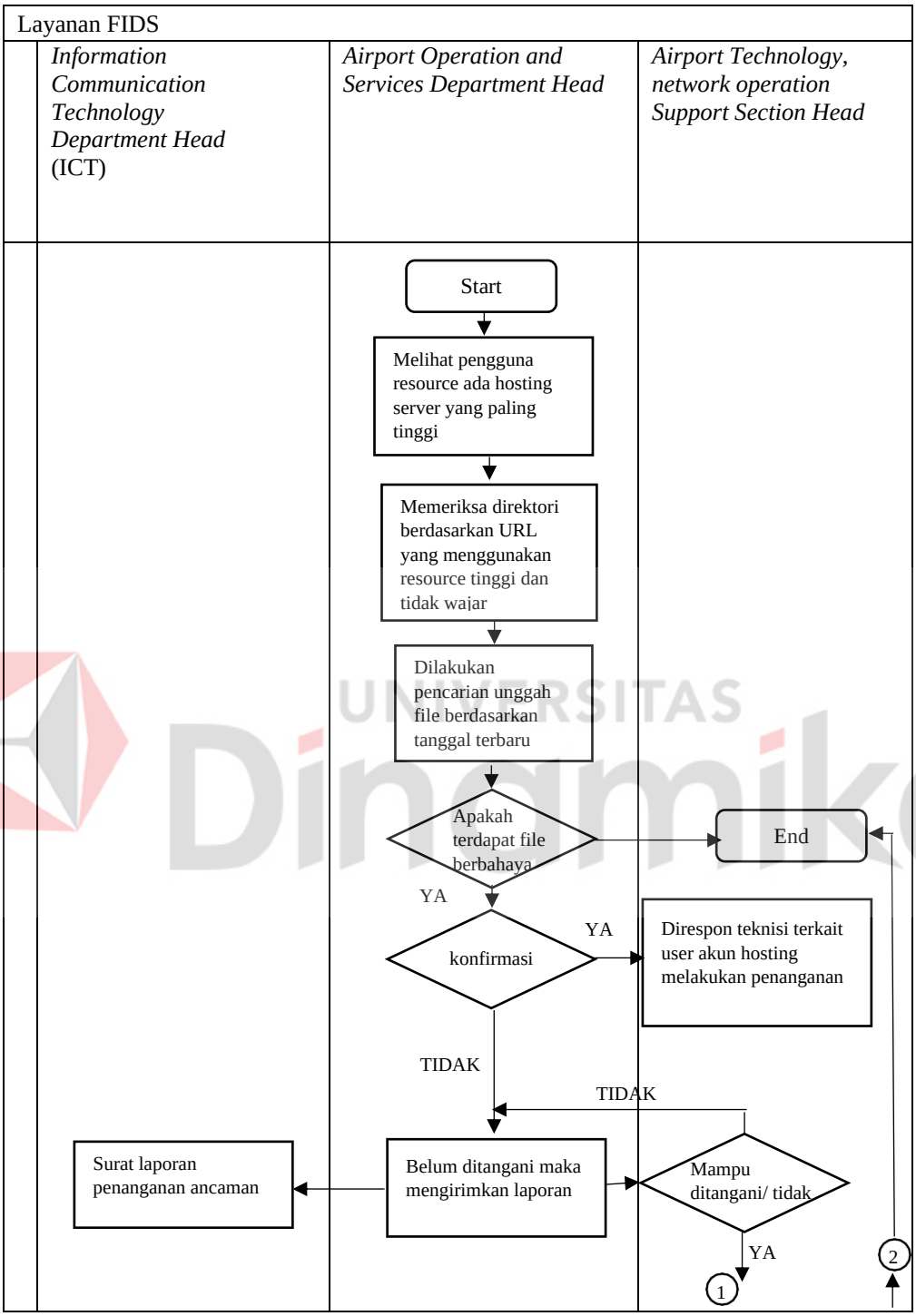


Lanjutan tabel lampiran 4

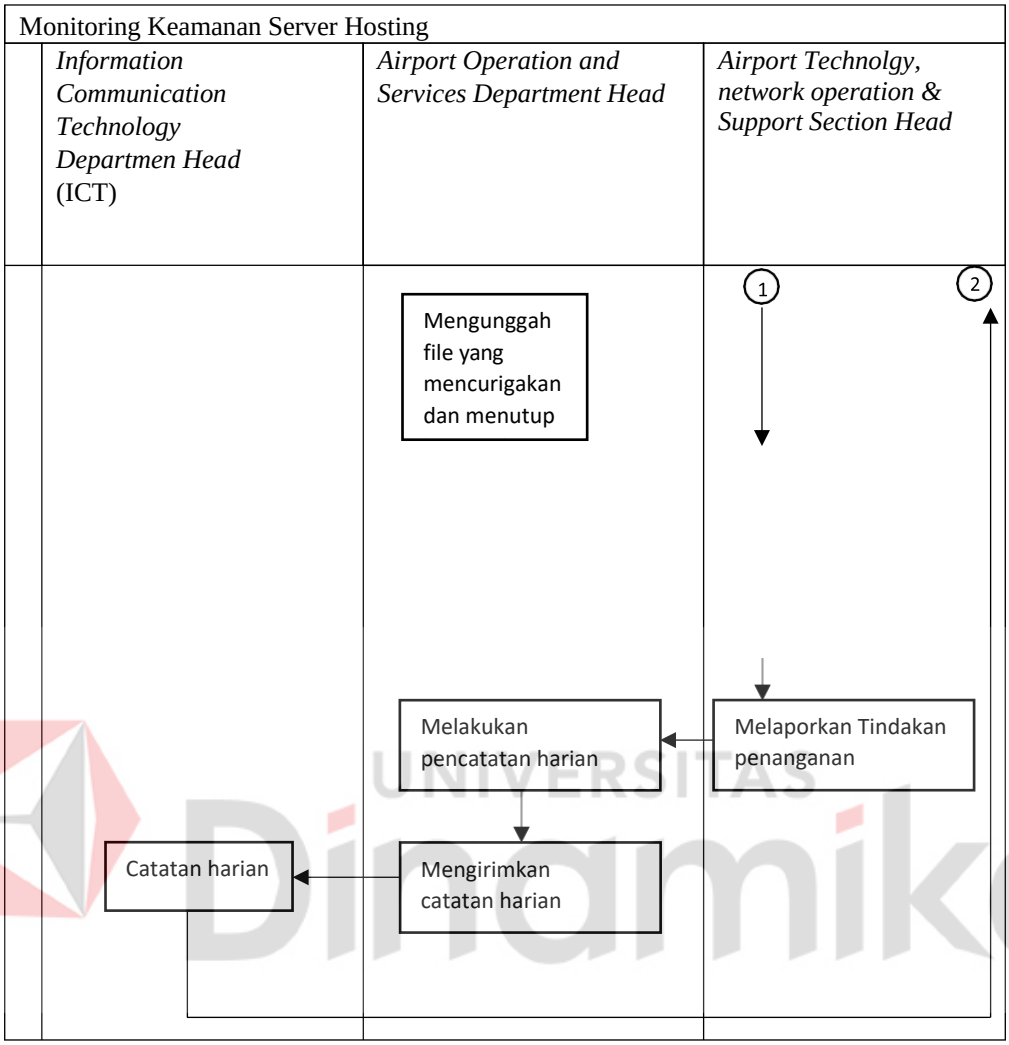


Lanjutan tabel lampiran 4





Lanjutan tabel lampiran 4



LAMPIRAN 5

DAFTAR KEJADIAN

No.	Tanggal	Kejadian	Tindakan	Laporan	Saran
1.	10-05-2020	*Mail server eror* status terjadi (*black mail* dan *spam mail*)	- Dalam kondisi normal status mail seperti ini adalah kematian layanan server, namun transaksi mail tetap normal - Dengan cek lebih dalam menggunakan *console* diketahui kalau servis normal, namun ada 1 server yang mati - Dengan matinya layanan ini, maka layanan lain tidak terpantau	- Dari hasil teknisi dilakukan *refreshing* dan memungkinkan untuk *restart* semua - Dari hasil akhir belum menunjukkan hasil yang memuaskan - Terjadinya perubahan *password* yang tidak tepat (tidak sesuai aturan)	
2.	10-05-2020	Kegagalan Ketika mengirim *email*	- Kembali menggunakan jaringan SMTP Telkom dengan konsekuensi kecepatan *mail* tergantung dari sistem Telkom	Mail menggunakan smtp sendiri. Penggunaan SMTP sendiri ini karena ada notifikasi dari pihak Telkom kalau IP mail telah di daftarkan PTR *record* mereka.	

3.	10-05-2020	Informasi yang tidak tampil dan belum ter *update*	- Dari server, file memang tidak ditemukan, kemungkinan terjadi kegagalan Ketika *upload* yang bisa disebabkan ketersediaan *bandwidth*		
4.	10-05-2020	Daftar agenda Sebagian tidak ter *update* dan tidak urut	- Memperbarui format - Memperbaiki form *input* - Menambahkan agenda - *Upload* ulang	Tampilan masih acak	
5.	10-05-2020	Data file yang diunggah tidak dapat tampil, informasi tidak ter *update*	- Menambahkan direktori didalamnya - Menambahkan ulang file	Adanya notifikasi file sukses di *upload* tetapi tidak dapat menampilkan file tersebut	

6.	11-05-2020	Serangan virus *ransomware*	- Melakukan *disable* SMB, *block* ip Port *ransomware* serta macro dalam upaya mencegah terjadinya Kembali virus *ransomware* dilingkup Angkasa Pura 1.	Penemuan FIDS yang terkena virus yang menyebabkan hilangnya data penerbangan	*Update antivirus* terbaru untuk *windows* SP sampai windows 11
7.	11-05-2020	Akses ilegal atau *hack device* pada FIDS	- Tahap awal menelusuri pada *system* yang terkena *hack* dan hasilnya ditemukan beberapa file dan direktori yang tidak seharusnya ada pada *system* tersebut.	Ditemukan *system* yang terkena hack, *system* ini di *hack* dan merubah tampilan pada *system* tersebut	- Harap meninjau halaman index - Hapus file-file yang tidak diperlukan - Menggunakan security *system* yang lebih baik
8.	2008	Tidak tersedianya informasi pengadaan fasilitas bandara	- Melakukan penelusuran pada sistem apakah terjadi akses ilegal/ pencurian data	Ditemukan sistem yang terkena *hack*, sistem di *hack* dan menghapus data informasi pengadaan fasilitas bandara	- Membuat dokumen kebijakan keamanan informasi

9.	2008	Hilang atau rusaknya informasi terkait hasil evaluasi tiap layanan bisnis utama	- Melakukan penelusuran pada sistem apakah terjadi akses ilegal/ pencurian data	Ditemukan sistem yang terkena *hack*, sistem di hack dan menghapus data informasi pengadaan fasilitas bandara	- Membuat dokumen kebijakan keamanan informasi
10.	2008	Pernah terjadi kehilangan atau kerusakan informasi terkait perencanaan pengadaan alat bagasi	- Melakukan penelusuran pada sistem apakah terjadi akses ilegal/ pencurian data	Ditemukan sistem yang terkena *hack*, sistem di *hack* dan menghapus data informasi pengadaan fasilitas bandara	- Membuat dokumen kebijakan keamanan informasi
11.	2008	Tidak tersedianya informasi operator garbarata	- Melakukan penelusuran pada sistem apakah terjadi akses ilegal/ pencurian data	Ditemukan sistem yang terkena *hack*, sistem di *hack* dan menghapus data informasi pengadaan fasilitas bandara	- Membuat dokumen kebijakan keamanan informasi

12.	2008	Tidak tersedianya informasi jadwal shift kerja pegawai	- Melakukan penelusuran pada sistem apakah terjadi akses ilegal/ pencurian data	Ditemukan sistem yang terkena *hack*, sistem di *hack* dan menghapus data informasi pengadaan fasilitas bandara	- Membuat dokumen kebijakan keamanan informasi
13.	2008	Pernah terjadi kehilangan informasi jadwal penerbangan	- Melakukan penelusuran pada sistem apakah terjadi akses ilegal/ pencurian data	Ditemukan sistem yang terkena *hack*, sistem di *hack* dan menghapus data informasi pengadaan fasilitas bandara	- Membuat dokumen kebijakan keamanan informasi
14.	2008	Rusak atau hilangnya data maskapai	- Melakukan penelusuran pada sistem apakah terjadi akses ilegal/ pencurian data	Ditemukan sistem yang terkena *hack*, sistem di *hack* dan menghapus data informasi pengadaan fasilitas bandara	- Membuat dokumen kebijakan keamanan informasi

LAMPIRAN 6

LANJUTAN LANDASAN TEORI

Lanjutan 2.3.2 Risiko Teknologi Informasi

tercakup dalam 6 kategori, yaitu:

1) Keamanan, yaitu informasi yang berisiko untuk diubah atau digunakan oleh pihak yang tidak berwenang.
2) Ketersediaan, yaitu data yang berisiko tidak dapat diakses setelah kegagalan sistem karena kesalahan manusia, aturan perusahaan, dan kurangnya pengurangan arsitektur.
3) Daya pulih, yaitu risiko dimana informasi yang diperlukan tidak dapat dipulihkan dalam waktu yang cukup setelah terjadinya kegagalan sistem.
4) Performance, yaitu risiko dimana informasi tidak tersedia saat diperlukan.
5) Daya Skala, yaitu risiko risiko yang perkembangan bisnis, pengaturan *bottleneck,* dan bentuk arsitekturnya membuat tidak mungkin menangani banyak aplikasi baru.
6) Ketaatan, yaitu risiko manajemen penggunaan informasi yang dapat melanggar keperluan dari pihak pemilik informasi.

Lanjutan 2.4 Metode OCTAVE

Fase 1: Melihat dari sisi organisasi

a. Proses
    1.) Mengidentifikasi berdasarkan pengetahuan pihak manajemen senior
    2.) Mengidentifikasi berdasarkan pengetahuan pihak manajemen operasional
    3.) Mengidentifikasi berdasarkan pengetahuan staff
    4.) Membuat profil ancaman
b. Output
    1.) Membuat daftar aset penting pada organisasi
    2.) Kebutuhan keamanan bagi aset organisasi
    3.) Daftar upaya untuk melindungi aset organisasi
    4.) Daftar ancaman terhadap aset kritis
    5.) Daftar kelemahan kebijakan organisasi

Fase 2: Melihat sisi teknologi

a. Proses
    1.) Melakukan identifikasi komponenS kunci
    2.) Evaluasi infrastruktur komponen
b. Output
    1.) Daftar komponen utama dan infrastruktur
    2.) Mendapatkan identifikasi kerentanan teknologi pada organisasi

Fase 3: Menganalisa risiko teknologi informasi

a. Proses
    1.) Melakukan analisa risiko
    2.) Mengembangkan strategi keamanan
b. Output
    1.) Daftar risiko terhadap aset kritis
    2.) Hasil pengukuran tingkat risiko
    3.) Strategi keamanan berdasarkan implementasi Octave
    4.) Rencana-rencana dari pengurangan atau mitigasi risiko

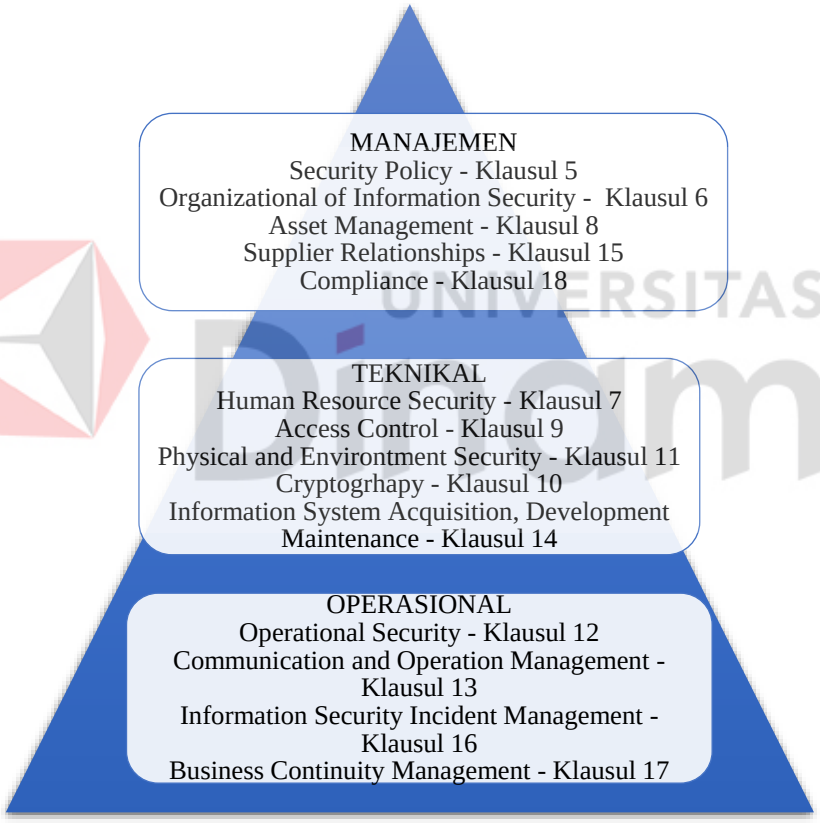
Lanjutan 2.5 Standar Sistem Manajemen Keamanan Informasi (SMKI)

Sistem Manajemen Keamanan informasi (SMKI) merupakan suatu proses yang disusun berdasarkan pendekatan risiko bisnis untuk merencanakan (*plan)*, mengimplementasikan *(do*), monitoring dan meninjau ulang (*check*) dan memelihara (*act*) terhadap keamanan informasi instansi [ISO/IEC 27001:2013]. Keamanan informasi ditujukan untuk menjaga aspek kerahasiaan (*confidentiality)*, keutuhan *(integrity*), dan ketersediaan (*availability*) dari informasi. (Sarno, 2009).

SMKI Berdasarkan ISO/IEC 27001:2013 menjelaskan syarat-syarat untuk membuat, menerapkan, melaksanakan, memonitor, menganalisa, dan memelihara serta mendokumentasikan sistem manajemen keamanan informasi (SMKI). ISO/IEC 27001 mendefinisikan keperluan-keperluan untuk sistem manajemen keamanan informasi yang baik membantu memberikan perlindungan terhadap gangguan pada aktivitas-aktivitas bisnis dan melindungi proses bisnis yang terpenting agar terhindar dari risiko kerugian/bencana dan kegagalan pada pengamanan informasi. ISO 27001 digunakan sebagai ikon sertifikasi ISO 27000.

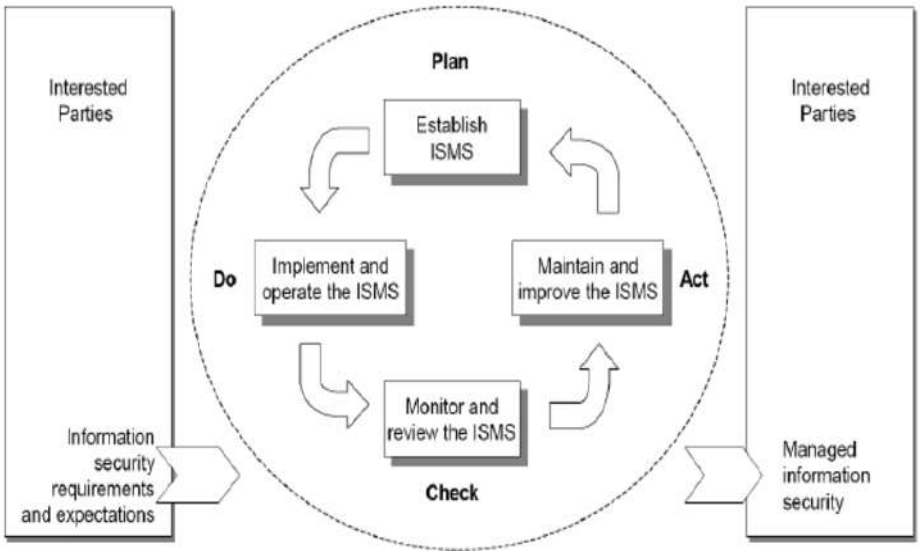
ISO 27000 merupakan dokumen standar sistem manajemen keamanan informasi yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah organisasi dalam usaha untuk mengimplementasikan konsep-konsep keamanan informasi dalam organisasi. (Sarno, 2009)

ISO/IEC 27001 berisi tentang panduan yang menjelaskan contoh penerapan keamanan informasi dengan menggunakan bentuk kontrol tertentu agar tercapainya sasaran kontrol yang ditetapkan. ISO/IEC 27001 memiliki 14 klausul, 35 kontrol objektif, dan 114 kontrol. Klausul-klausul tersebut dapat dikelompokkan menjadi tiga kebutuhan kontrol keamanan, yaitu manajerial, teknikal dan operasional yang dapat di gambarkan dalam hubungan piramida seperti Gambar 2.7 1.



Gambar 2.5 1 - Kelompok Kontrol Keamanan

Lanjutan 2.6 Model Proses



Gambar 2.5 Model PDCA (Sarno, 2009)

Gambar 2.5 merupakan model PDCA yang terdapat pada ISO 27001 yang dijelaskan sebagai berikut:

1. *Plan*

   Tahapan ini merupakan kegiatan perencanaan dan perancangan Sistem Manajemen Keamanan Informasi (SMKI). Pada tatanan implementasinya adalah membangun komitmen, kebijakan, kontrol, prosedur, instruksi kerja dan lain-lain sehingga tercipta SMKI sesuai dengan kebutuhan.

2. *Do*

   Tahapan ini merupakan tahap implementasi dari kebijakan, kontrol, proses dan prosedur SMKI yang telah direncanakan pada tahap *plan.*

3. *Check*

   Tahap ini membahas mengenai kegiatan pemonitoran pelaksanaan SMKI, termasuk melakukan evaluasi dan audit SMKI.

4. *Act*

   Tindakan korektif dan pencegahan berdasarkan hasil internal audit SMKI dan tinjauan manajemen atau informasi terkait lainnya untuk mencapai perbaikan berkesinambungan dalam SMKI.

2.8 Lanjutan 2.8.1 Pemetaan Kontrol Objektif

Tabel 2.8-1 – Pemetaan Kontrol Objektif berdasarkan *Secure Online Business* (Jolly, 2003)

No.	ISO 27001: 2013	Contents
1.	Klausul 5: Kebijakan Keamanan Informasi Klausul 8: Manajemen Asset Klausul 11: Keamanan Fisik Dan Lingkungan Klausul 18: Kesesuaian	Kebijakan Keamanan
2.	Klausul 6: Organisasi Keamanan Informasi Kontrol Objektif: 6.2 Kontrol Keamanan: 6.2.2	Bekerja Jarak Jauh
3.	Klausul 7: Keamanan Sumber Daya Manusia	Pengendalian Musuh Internal
		Kerahasiaan SDM dan Budaya Keamanan
4.	Klausul 9: Kontrol Akses Kontrol Objektif: 9.2 Kontol Keamanan: 9.2.4	*Otentikasi* dan *Enkripsi*
	Klausul 10: Kriptografi	
5.	Klausul 9: Kontrol Akses	Jaringan
	Klausul 13: Keamanan Komunikasi	
	Klausul 14: Sistem Akuisisi, Pengembangan Dan Pemeliharaan	
6.	Klausul 12: Keamanan Operasi Kontrol Objektif: 12.2 Kontrol Keamanan: 12.2.1	Data Recovery
7.	Klausul 13: Keamanan Komunikasi Kontrol Objektif: 13.2 Kontrol Keamanan: 13.2.3	*Email*
8.	Klausul 14: Sistem Akuisisi, Pengembangan Dan Pemeliharaan	Perlindungan Perangkat Lunak
9.	Klausul 15: Manajemen Penyampaian Layanan Pemasok	Manajemen Layanan Keamanan
10.	Klausul 16: Informasi Manajemen Insiden Keamanan	Risiko Informasi
11.	Klausul 17: Aspek Keamanan Informasi Manajemen Kontinuitas Bisnis	Manajemen Kelangsungan Bisnis

Dalam tabel pemetaan kontrol objektif berdasarkan Secure Online Business (Jolly, 2003) tersebut adapun penanganan teknis yang tertulis pada table 2.8 1

Tabel 2.8 2 – Penanganan Teknis (Jolly, 2003)

No.	Contents	Penanganan Teknis
1.	Kebijakan Keamanan	- Data dan Informasi - Aset organisasi - Hukum - *Cybercrime*: Perlindungan data, *Whistle-blowing* kebijakan
2.	Bekerja Jarak Jauh	- Teknik koneksi *dial-up point-to point* - *Business* internet-driven - VPN (Virtual Private Network) - *Teleworkers*
3.	Pengendalian Musuh Internal	- Pegawai/SDM - *Password* - *Virus* - Kejahatan internet - *E-mail* - Jaringan
	Kerahasiaan SDM dan Budaya Keamanan	- Teknik rekrutmen *outsourcing* (kontrak kerja dan kebijakan), pelatihan
4.	*Otentikasi* dan *Enkripsi*	- *Otentikasi: password* - Privasi data: *Secure Socket Layer* (SSL) - *Integrasi*: sertifikat digital (identitas fisik dan identitas digital), Kriptografi - Otorisasi: URL, akses kontrol
5.	Jaringan	- Teknik keamanan *software*: *firewall* dan fungsi enkripsi VPN (*Virtual Private Network*), VLAN - Teknik penolakan layanan - Pencegahan intrusi / deteksi jaringan
6.	Data *Recovery*	- *Back-up* - Merekam file - Simpan dalam *harddisk*
7.	*Email*	- Enkripsi data - Enkripsi teknik anti-virus - Tanda tangan digital / teknik kriptografi

8.	Perlindungan Perangkat Lunak	- Deteksi gangguan: *Intrusion Detection Systems* (IDS) - *Firewall*: IP, filter paket berdasarkan jenis data atau TCP/IP nomor *port*, aplikasi *proxy* - Virus: *software* anti-virus - *Otentikasi* dan *enkripsi* - Manajemen Hak digital dan Lisensi *elektronik*: teknik DMR
9.	Manajemen Layanan Keamanan	- *Service-level agreements* (SLA) - *Network operations center* (NOC)
10.	Risiko Informasi	- Menghitung probabilitas dampak informasi - Menghitung *Return on Investment* (ROI)
11.	Manajemen Kelangsungan Bisnis	- Teknik Strategi *Business Continuity Management* (BCM) - Strategi kelangsungan bisnis: Tahap 0: Perencanaan Pra-Proyek Tahap 1: Penilaian Tahap 2: Desain Tahap 3: Pelaksanaan Tahap 4: Pengujian, pemeliharaan dan perbaikan

Adapun penjelasan dari penanganan teknis pada tabel 2.8 sebagai berikut:

1. Kebijakan *Whistle-blowing* yaitu sistem pelaporan pelanggaran yang memungkinkan setiap orang untuk melaporkan adanya dugaan tindakan kecurangan, pelanggaran hukum, etika, dan kode etik instansi yang dilakukan oleh pegawai.
2. Teknik koneksi *dial-up-point-to-point* yaitu metode yang menghubungkan pekerjaan jarak melalui internet
3. *Virtual Private Network* (VPN) *Teleworkers* yaitu teknik menghubungkan jaringan jarak jauh instansi dan mengakses sistem bisnis dan informasi yang penting
4. *Virtual Private Network* (VPN) yaitu jaringan pribadi virtual keamanan antara dua titik, antara kantor pusat jaringan instansi dan kantor cabang terpencil. Melewati *enkripsi* data melalui internet publik, kemudian mendeskripsikan

itu pada titik tujuan dan melindungi data dari *hacker* pada jalurnya melalui internet, dan membuat data tidak terbaca selama proses pegiriman

5. *Secure Socket Layer* (SSL) yaitu kemampuan untuk memastikan privasi informasi yang ditransfer antara *web* dan *web browser* pengguna. Hal ini dilakukan dengan mengenkripsi informasi sebelum mengirimnya dan kemudian mendeskripsikan kepada penerima, sehingga hampir tidak mungkin untuk diterjemahkan jika terjadi kecurangan.
6. Sertifikat Digital (identitas fisik dan identitas digital) yaitu sebagai bentuk otentikasi dalam pertumbuhan transaksi internet. Sertifikat digital membantu mengidentifikasi pengguna dengan mengharuskan untuk mengakses kredensial digital yang seharusnya hanya digunakan oleh pemilik yang sah.
7. Akses bersyarat yaitu sebuah direktori dari file berdasarkan daftar kontrol akses yang bertujuan untuk mengakses data pengguna atau sumber daya yang dilindungi
8. Teknik penolakan layanan yaitu serangan berbasis *hacker* pada *web server* yang mencegah pelanggan/ pengunjung dari mendapatkan akses situs web organisasi. Biasanya diluncurkan oleh virus worm (misalnya *code red, code blue*) yang dapat mereplika dari komputer ke komputer. Ada juga '*distributed denial of service'* serangan, yang secara bersamaan menyerang beberapa *server* sekaligus.
9. Pencegahan instruksi / deteksi jaringan yaitu aplikasi yang memberikan alarm operator pencegahan interupsi. Hal ini juga memiliki kemampuan untuk menjatuhkan serangan dari jaringan untuk menghentikannya dari mencapai target.
10. *Backdoor* atau *U-turn* yaitu metode serangan jaringan yang bertujuan untuk kantor cabang kecil yang memiliki akses internet baik lokal maupun melalui VPN instansi masuk secara ilegal diperoleh melalui link lokal dan, sekali di balik situs *remote* VPN
11. Enkripsi *email* yaitu metode praktis untuk memastikan bahwa informasi yang berkaitan dengan out-of-date yang sudah kadaluwarsa di catatan dan dibuang dengan benar.

12. Tanda tangan digital yaitu cara penandatanganan dan penyegelan elektronik yang terintegrasi dan menggunakan kriptografi kunci publik. Sebuah email yang telah ditandatangani secara digital memastikan bahwa pesan tidak dapat ditolak atau dianggap tidak sah (ditolak oleh pengirim).
13. *Intrusion Detection System* (IDS) yaitu memberikan arahan untuk mendeteksi sistem dalam menyediakan kesempatan yang ideal untuk mengelola dan mengevaluasi layanan keamanan jaringan tanpa menimbulkan risiko biaya besar.
14. Filter paket yaitu jenis yang paling dasar dari *firewall* dan sering gratis dan tersedia pada router populer. Sebuah filter paket hanya memeriksa alamat IP daftar kontrol akses (ACL). Dan menolak akses ke alamat yang tidak sesuai dengan data atau TCP / IP (transmisi protokol kontrol / protokol Internet) nomor port.
15. Infrastruktur kunci dan publik (IPK) yaitu sebuah cara untuk menarik atau meningkatnya minat dari jumlah instansi besar dan menengah dan organisasi, sebagai penyedia layanan untuk memperoleh keuntungan strategis dan financial.
16. Management Hak digital dan Lisensi elektronik: teknik DMR yaitu sebuah lisensi atau hak cipta elektronik untuk aplikasi yang diberikan langsung atau dalam pengembangan yang masih mempertahankan hak akses penuh kapan atas bagaimana dan kapan merekan dapat membuka aplikasi tersebut melalui lisensi elektronik.
17. *Service-level agreements* (SLA) yaitu komponen kunci tujuan dan sasaran dari pemasok dan klien bersama yang bertujuan untuk memberikan pelayanan keamanan yang memenuhi bisnis dan persyaratan teknis yang telah disepakati.
18. *Network operations center* (NOC) yaitu merupakan indikasi bahwa penyedia layanan pemilik pusat operasi keamanan jaringan (memantau, mengelola, dan mengatur).
19. Menghitung *Return on Investment* (ROI) yaitu cara analisa biaya/risiko atau manfaat yang komprehensif untuk setiap pengeluaran keamanan.

20. Teknik Strategi *Business Continuity Management* (BCM) yaitu suatu proses mengidentifikasi potensi dampak yang mengancam organisasi dan menyediakan kerangka kerja untuk membangun ketahanan dan kemampuan untuk respon yang efektif melindungi kepentingan *stakeholder*, reputasi organisasi, brand, dan kegiatan penciptaan nilai.
21. Strategi kelangsungan bisnis yaitu strategi untuk mencapai BCM yang dibagi dengan 5 tahap.

Pemetaan ISO 27001:2013 dengan content buku *Secure Online Business* (Jolly, 2003) bertujuan untuk mempermudah memberikan penanganan dari hasil pengelolaan risiko keamanan informasi secara teknis.

2.9 Lanjutan Standar Operational Procedure (SOP)

Dokumen Standr Operating Procedure

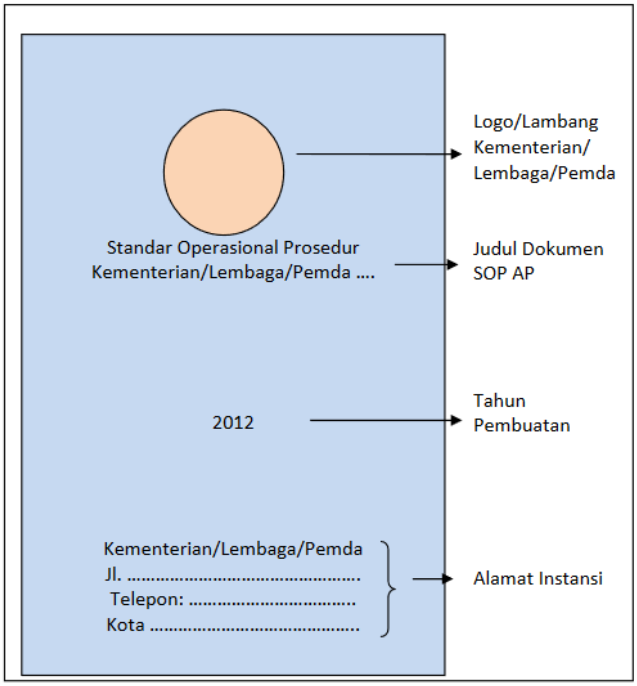
dalam penyusunan dokumen SOP, menurut peraturan pemerintah (Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia, 2012) didasarkan pada format SOP yang telah disusun. Namun tidakbakuan format SOP menyebabkan organisasi dapat menyusun dokumen SOP sesuai dengan kebutuhannya masing-masing. Format SOP dipengaruhi oleh tujuan pembutan SOP. Sehingga apabila tujuan pembuatan SOP maka format SOP juga dapat berbeda.

Sesuai dengan anatomi dokumen SOP yang pada hakekatnya berisi prosedur-prosedur yang distandarkan dan membentuk satu kesatuan proses, maka informasi yang dimuat dalam dokumen SOP terdiri dari 2 macam unsur, yaitu unsur dokumentasi dan unsur prosedur. Adapun informasi yang terdapat dalam unsur dokumentasi dan unsur prosedur adalah:

1. Unsur Dokumentasi

Unsur dokumentasi merupakan unsur dari dokumen SOP yang berisi hal-hal yang terkait dengan proses pendokumentasian SOP sebagai sebuah dokumen.

Berikut adalah contoh halaman judul sebuah dokumen SOP yang dapat dilihat pada Gambar 2.8.



Gambar 2.9 Contoh Halaman Judul Dokumen SOP

ruang lingkup yang berisi penjelasan tujuan pembuatan prosedur, ringkasan yang berisi ringkasan singkat mengenai prosedur dan definisi umum yang berisi beberapa definisi yang terkait dengan prosedur yang distandarkan.

2. Unsur Prosedur

Unsur prosedur merupakan unsur dari dokumen SOP yang berisi hal-hal inti dari dokumen SOP. Unsur prosedur dibagi dalam dua bagian, yaitu Bagian Identitas dan Bagian *Flowchart*. Adapun penjelasan unsur prosedur adalah:

a. Bagian identitas

Bagian identitas dari unsur prosedur dalam SOP dapat dilihat pada Gambar 2.9-1.

KEMENTERIAN PENDAYAGUNAAN APARATUR NEGARA DAN REFORMASI BIROKRASI DEPUTI BIDANG TATALAKSANA ASISTEN DEPUTI PENGEMBANGAN SISTEM DAN PROSEDUR PEMERINTAHAN		
	NOMOR SOP	: K/PAN-RB/D.IV/4/001/2011
	TGL. PEMBUATAN	: 6 Juli 2011
	TGL. REVISI	:
	TGL. EFEKTIF	: 8 Agustus 2011
	DISAHKAN OLEH	: Asisten Deputi Pengembangan Sistem dan Prosedur Pemerintahan Nama NIP
	NAMA SOP	: PEMBUATAN LAPORAN KONSINYERING

DASAR HUKUM:	KUALIFIKASI PELAKSANA:
1. Peraturan Presiden Republik Indonesia Nomor 47 Tahun 2009 tentang Pembentukan dan Organisasi Kementerian Negara 2. Peraturan Presiden Republik Indonesia Nomor 24 Tahun 2010 tentang Kedudukan, Tugas, dan Fungsi Kementerian Negara serta Susunan Organisasi, Tugas, dan Fungsi Eselon I Kementerian Negara 3. Peraturan Menteri Negara PAN dan RB Nomor 12 Tahun 2010 tentang Organisasi Dan Tata Kerja Kementerian PAN dan RB	1. Memiliki kemampuan pengolahan data sederhana 2. Mengetahui tugas dan fungsi Sistem dan Prosedur Pemerintahan 3. Mengetahui tugas dan fungsi mekanisme pembuatan laporan
KETERKAITAN:	**PERALATAN/PERLENGKAPAN:**
1. SOP Pelaksanaan Konsinyering 2. SOP Pendokumentasian Laporan Konsinyering 3. SOP Pencairan Anggaran Konsinyering	1. Lembar Kerja / Rencana Kerja dan Anggaran 2. Term of Refference 3. Komputer/Printer/Scanner 4. Jaringan internet
PERINGATAN:	**PENCATATAN DAN PENDATAAN:**
Apabila Laporan Konsinyering terlambat dibuat maka pelaksanaan kegatan Konsinyering berikutnya akan tertunda.	- Di simpan sebagai data elektronik dan manual

Gambar 2.9.1 Contoh Bagan Identitas SOP

(Sumber: Pedoman Penyusunan SOP Administrasi Pemerintahan Tahun 2012)

b. Bagian *Flowchart*

Bagian Flowchart merupakan uraian mengenai langkah-langkah(prosedur) kegiatan beserta mutu baku dan keterangan yang diperlukan. Bagian *Flowchart* Ini berupa *flowcharts* yang menjelaskan langkah-langkah kegiatan secara berurutan dan sistematis. Berikut adalah contoh bagian *flowchart* SOP yang dapat dilihat pada Tabel 2.9-2.

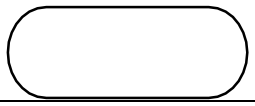
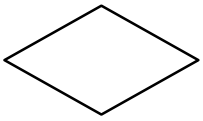
Gambar 2.9 -2 Contoh Bagan Flowchart SOP

(Sumber: Pedoman penyusunan SOP Administrasi Pemerintahan, 2012)

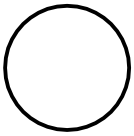
No.	Kegiatan	Pelaksana				Mutu Baku			Keterangan
		Kabid	Kasubid	Analis	Asdep	Kelengkapan	Waktu	Output	
1.	Menugaskan Kasubid untuk mempersiapkan konsep laporan konsinyering					Agenda Kerja	15 menit	Disposisi	
2.	Memerintahkan analis untuk mengumpulkan bahan laporan konsinyering					Disposisi	15 menit	Disposisi	
3.	Mengumpulkan dan menyerahkan bahan konsinyering kepada Kasubid					Disposisi	1 hari	Bahan Laporan, Disposisi	SOP Pengumpul-an Bahan
4.	Mengonsep laporan konsinyering dan menyerahkan kepada Kabid					Bahan Laporan	2 jam	Konsep Laporan, Disposisi	
5.	Memeriksa konsep laporan konsinyering. Jika setuju menyampaikan kepada Asdep. Jika tidak setuju menyerahkan kepada Kasubid untuk diperbaiki.	Tidak / Ya				Konsep Laporan	1 jam	Draft Laporan, Disposisi	
6.	Memeriksa draft laporan konsinyering. Jika setuju menandatangani dan menyerahkan kepada Kabid. Jika tidak setuju mengembalikan kepada Kabid untuk diperbaiki.				Tidak / Ya	Draft Laporan	1 jam	Laporan, Disposisi	
7.	Menyerahkan laporan konsinyering kepada Kasubdit untuk didokumentasikan.					Laporan	10 menit	Disposisi	
8.	Menyerahkan laporan konsinyering kepada Analis untuk didokumentasikan.					Laporan	10 menit	Disposisi	
9.	Mendokumentasikan Laporan Konsinyering					Laporan	15 menit	Laporan, Bukti Dokumentasi	

Simbol-simbol pada bagian *flowchart* SOP dapat dilihat pada Tabel 2.9 3

Tabel 2.9 3 Penjelasan Simbol *flowchart* SOP

No	Simbol	Nama	Fungsi
1		Terminal	Memulai dan mengakhiri sebuah proses
2		Proses	Aktivitas yang dilakukan sebuah fungsi/unit kerja/jabatan, bisa berupa kegiatan atau perhitungan. Proses ini menghasilkan barang, jasa, konsep, dokumen, saran, dan sebagainya.
3		Keputusan	Menggambarkan proses pengambilan keputusan yang diambil oleh unit / kerja/ jabatan. Hasilnya bisa berupa “Ya” atau “Tidak”.

Lanjutan tabel 2.9.3

4		Dokumen	Data yang berbentuk informasi, bisa dalam bentuk dokumen tertulis atau file komputer. Bisa merupakan hasil sebuah proses, atau merupakan masukan proses.
5		Penghubung	Penghubung digunakan jika diagram alir tidak dapat ditampung dalam satu bagian atau satu halaman, menunjukkan menyambungkan ke bagian lain atau halaman lain.
6		Anak Panah	Menunjukkan arah aliran dari suatu kegiatan ke kegiatan lain, atau menunjukkan arah pilihan yang dapat diambil.

Lanjutan 2.9 poin C.

1. Metode *Risk Assessment*: Metode yang digunakan untuk melakukan penilaian risiko terhadap informasi dapat dilakukan dengan beberapa metode antara lain: metode statistik atau metode matematis.
2. Kriteria penerimaan risiko: Kriteria penerimaan risiko ditujukan sebagai acuan tindakan yang dilakukan dalam menangani risiko yang ada dalam organisasi (Sarno, 2009). Metode ini menentukan kriteria penerimaan risiko dapat menggunakan tabel matriks 3x3 yang merupakan hubungan variabel sebagai berikut:
    1) Probabilitas ancaman
    2) Biaya pemulihan akibat atau karena dampak dari penerimaan risiko.
    3) Biaya transfer risiko kepada pihak ketiga

2.9 Poin D (Lanjutan) langkah-langkah untuk mengidentifikasi risiko

1) Mengidentifikasi aset

Mengidentifikasi aset dan klasifikasi aset sesuai dengan ruang lingkup dalam SMKI dapat dilakukan dengan menggunakan tabel aset yang telah dikategorikan menurut jenis atau kebutuhan organisasi. (Sarno, 2009). Menghitung nilai aset

Cara menghitung nilai aset yang dimiliki organisasi berdasarkan aset keamanan informasi yaitu *Confidentiality*, *Integrity*, dan *Availability* dapat menggunakan contoh tabel penilaian aset berdasarkan kriteria *Confidentiality* yang ditunjukkan pada tabel 2.5. (Sarno, 2009).

Tabel 2.10-1 – Contoh Penilaian Aset berdasarkan Kriteria *Confidentiality*

(Sumber Sarno, 2009)

Kriteria *Confidentiality*	Nilai *Confidentiality* (NC)
Public	0
Internal use only	1
Private	2
Confidential	3
Secret	4

Kriteria nilai *Integrity* ditunjukkan pada tabel 2.10-2

Tabel 2.10-2 – Contoh Penilaian Aset berdasarkan Kriteria *Integrity*

(Sumber: Sarno, 2009)

Kriteria *Integrity*	Nilai *Integrity* (NI)
No Impact	0
Minor incident	1
General disturbance	2
Mayor disturbance	3
Unacceptable damage	4

Kriteria nilai *Availability* ditunjukkan pada tabel 2.10-3

Tabel 2.10-3 – Contoh Penilaian Aset berdasarkan Kriteria *Availability*

(Sumber Sarno, 2009)

Kriteria *Availability*	Nilai *Availability* (NV)
No Availability	0
Office hours Availability	1
Strong Availability	2

High Availability	3
Very High Availability	4

Perhitungan nilai aset dapat dihitung dengan menggunakan persamaan matematis berikut:

Nilai Aset (NA)= NC + NI + NV.....(G.1)

dimana:

NC = Nilai *Confidentiality*

NI = Nilai *Integrity*

NV = Nilai *Availability*

2) Mengidentifikasi ancaman *(threat)* dan kelemahan *(vulnerability* yang dimiliki oleh aset mengidentifikasi ancaman dan kelemahan terhadap aset dapat menggunakan tabel *probability of Occurrence* dengan menentukan rentang nilai *probability* dari level *LOW, MEDIUM,* dan *HIGH*. (Sarno, 2009).

Tabel 2.10-4 – Contoh Kemungkinan Gangguan Keamanan
(Sumber: Sarno, 2009)

No	Kejadian	Jenis	*Probabilitas*	Rerata *Probabilitas*
1.	Gangguan Sumber Daya	Kelemahan	Low	0,1
2.	Gangguan Perangkat Keras	Kelemahan	Medium	0,4
3.	Bencana Alam	Ancaman	Low	0,2
4.	Akses Ilegal	Ancaman	Medium	0,6
5.	Virus *Attack*	Ancaman	High	0,7

Nilai rerata *probabilitas* didapatkan dari hasil klasifikasi probabilitas dengan rentang nilai yang dapat didefinisikan sebagai berikut:

1. *LOW* : nilai rerata *probabilitas* 0,1-0,3
2. *MEDIUM* : nilai rerata probabilitas 0,4-0,6

3. *HIGH* : nilai rerata probabilitas 0,7-1,0

Rumus yang digunakan untuk menghitung nilai ancaman (*threat*) dan kelemahan (*Vulnerable*) dari suatu aset yaitu:

Nilai Ancaman (NT) = ∑ PO / ∑ Ancaman.....(G.2)

Dimana:

∑ PO : jumlah *Probability of Occurrence*

/ ∑ Ancaman : jumlah ancaman terhadap informasi

Tabel 2.10-5 – Contoh menghitung nilai ancaman

(Sumber Sarno, 2009)

No	Ancaman	Jenis	*Probabilitas*	Rerata *Probabilitas*
1.	Gangguan Sumber Daya	Kelemahan	*Low*	0,1
2.	Gangguan Perangkat Keras	Kelemahan	*Medium*	0,4
3.	Bencana Alam	Ancaman	*Low*	0,2
4.	Akses *Ilegal*	Ancaman	*Medium*	0,6
5.	Virus *Attack*	Ancaman	*High*	0,7
	□ Ancaman = 5	□ PO		2.0

Nilai ancaman (server) = ∑PO / ∑Ancaman = 2,0/5 = 0,4

3) Identifikasi dampak *(impact*) jika terjadi kegagalan penjagaan aspek keamanan informasi (CIA) yaitu mengidentifikasi dampak bisnis yang terjadi kegagalan penjagaan terhadap aspek-aspek keamanan informasi. Tujuannya adalah untuk melihat bagaimana dampak terhadap organisasi jika terjadi kegagalan.

2.10 Lanjutan poin E Analisa dan evaluasi risiko

1) melakukan analisa dampak bisnis

Analisa dampak bisnis adalah analisa yang menggambarkan seberapa tahan proses bisnis di dalam organisasi berjalan ketika informasi yang dimiliki terganggu dengan menentukan nilai BIA pada masing-masing aset (Sarno, 2009). Skala nilai BIA digunakan untuk menentukan nilai BIA yang ditunjukkan pada tabel 2.10- 6

Tabel 2.10-6 – Skala Nilai BIA
(Sumber Sarno, 2009)

Batas Toleransi gangguan	Keterangan	Nilai BIA	Nilai Skala
< 1 minggu	*No Critical*	0	0-20
1 hari s/d 2 hari	*Minor critical*	1	21-40
<1 hari	*Mayor critical*	2	41-60
<12 jam	*High critical*	3	61-80
< 1 jam	*Very high critical*	4	81-100

2) mengidentifikasi level risiko

level risiko adalah tingkat risiko yang timbul jika dihubungkan dengan dampak dan probabilitas ancaman yang mungkin timbul. Mengidentifikasi level risiko dapat dibuat menggunakan matriks level risiko sesuai dengan menggunakan nilai-nilai *probabilitas* ancaman yang telah ditentukan. Identifikasi level risiko dapat digambarkan dalam bentuk matriks level risiko yang di tunjukkan pada tabel 2.10-7

Tabel 2.10-7 – Matriks Level Risiko
(Sumber Sarno, 2009)

Probabilitas Ancaman	Dampak Bisnis				
	Not Critical (20)	*Low Critical* (40)	*Medium Critical* (60)	*High Critical* (80)	*Very High Critical* (100)
Low (0,1)	*Low* 20x0,1=2	*Low* 40x0,1=4	*Low* 60x0,1=6	*Low* 80x0,1=8	*Low* 100x0,1=10
Medium (0,5)	*Low* 20x0,5=10	*Medium* 40x0,5=20	*Medium* 60x0,5=30	*Medium* 80x0,5=40	*Medium* 100x0,5=50
High (1,0)	*Medium* 20x1,0=20	*Medium* 40x1,0=40	*High* 60x1,0=60	*High* 80x1,0=80	*High* 100x1,0=100

3) menentukan risiko diterima atau perlu pengelolaan risiko dalam penentuan apakah risiko diterima atau masih membutuhkan pengelolaan risiko berdasarkan kriteria penerimaan risiko. Untuk menentukan level risiko diperlukan nilai risiko untuk menentukan letak level dari masing-masing aset yaitu dengan menggunakan perhitungan persamaan matematis berikut:

Nilai Risiko (*Risk Value*) = NA x BIA x NT

.....

dimana:

NA : Nilai Aset

BIA : Analisa Dampak Bisnis (*Business Impact Analysis*)

NT : Nilai Ancaman (*Nilai Threat*)

2.10 **Lanjutan poin G memilih kontrol objéktif dan kontrol untuk pengelolaan risiko (*risk mitigation)***

1. Klausul 5 : Kebijakan Keamanan Informasi (*Information Security Policies*)
2. Klausul 6 : Organisasi Keamanan Informasi (*Organization of Information Security*)
3. Klausul 7 : Keamanan Sumber Daya Manusia (*Human Resource Security*)
4. Klausul 8 : Manajemen Asset (*Asset Management*)
5. Klausul 9 : Kontrol Akses (*Access Control*)
6. Klausul 10 : Kriptografi (*Cryptography*)
7. Klausul 11 : Keamanan Fisik Dan Lingkungan (*Physical and Environmental Security*)
8. Klausul 12 : Keamanan Operasi (*Operations Security*)
9. Klausul 13 : Keamanan Komunikasi (*Communication Security*)
10. Klausul 14 : Sistem Akuisisi, Pengembangan Dan Pemeliharaan (*System Acquisition, Development and Maintenance*)
11. Klausul 15 : Manajemen Penyampaian Layanan Pemasok (*Supplier Relationships*)

12 Klausul 16 : Informasi Manajemen Insiden Keamanan (*Information Security Incident Management*)

13. Klausul 17 : Aspek Keamanan Informasi Manajemen Kontinuitas Bisnis (*Information Security Aspects of Business Continuity Management*)

14 Klausul 18 : Kesesuaian (*Compliance*)

2.10 Lanjutan poin H Pengelompokan kebutuhan kontrol objektif

Tabel 2.10 – 8 Kebutuhan Kontrol Objektif

(Sumber Sarno, 2009)

Kategori Kebutuhan	No. Klausul	Klausul	Kontrol Objektif
Manajemen/Organisasi	5	Kebijakan Keamanan	Manajemen Kebijakan Keamanan Informasi
	6	Organisasi Keamanan Informasi	Organisasi Internal Keamanan Informasi
			Perangkat *mobile* dan *Teleworking*
	8	Manajemen aset	Tanggung jawab aset
			Informasi klasifikasi
			Penanganan media
Teknikal	18	Kesesuaian	Kepatuhan terhadap persyaratan hukum dan kontrak
			Tinjauan keamanan Informasi
	7	Keamanan sumber daya manusia	Keamanan SDM sebelum menjadi Pegawai
			Keamanan SDM selama menjadi Pegawai
			Pemberhentian atau pemindahan pegawai

	9	Kontrol Akses	Persyaratan bisnis pengendalian akses
			Manajemen akses Pengguna
			Tanggung jawab Pengguna
			Kontrol akses sistem dan aplikasi
	10	Kriptografi	Kontrol kriptografi
	11	Keamanan fisik dan lingkungan	Keamanan area/wilayah
			Keamanan peralatan
	14	Akuisisi, pengembangan dan pemeliharaan sistem	Persyaratan keamanan sistem informasi
			Keamanan dalam proses pengembangan dan pendukung
			Uji data
Operasional	12	Keamanan operasi	Prosedur dan tanggung jawab operasional
			Proteksi dari malware
			Backup
			Pengembangan dan pemantauan
			Pengendalian perangkat lunak operasional
			Pengelolaan kerentanan teknis
			Pertimbangan audit sistem informasi
	13	Keamanan komunikasi	Manajemen keamanan jaringan
			Transfer informasi
	17	Aspek keamanan informasi manajemen kelangsungan bisnis	keamanan informasi kelangsungan bisnis
		Hubungan pemasok	Redundansi

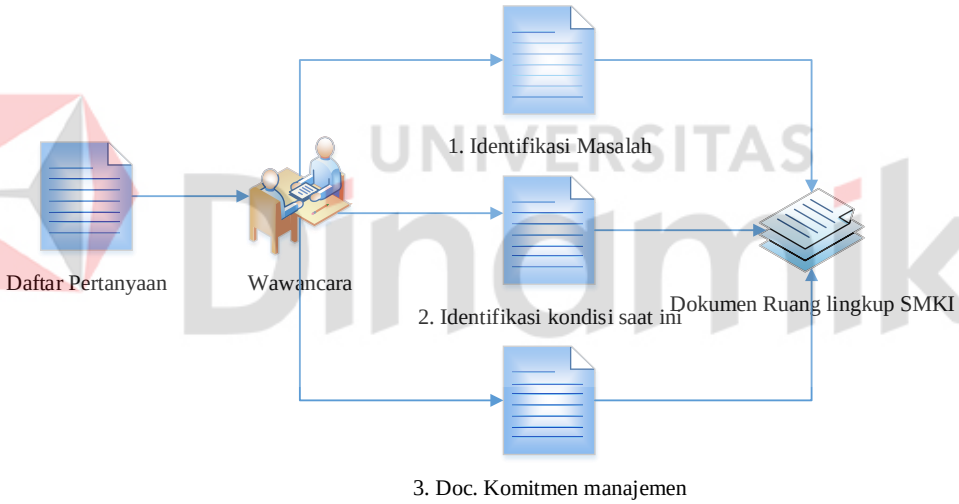
	15		Keamanan informasi dalam hubungan pemasok
Operasional	16	Manajemen insiden keamanan informasi	Manajemen penyampaian layanan pemasok
			Pengelolaan insiden dan perbaikan keamanan informasi

LAMPIRAN 7

LANJUTAN METODOLOGI PENELITIAN

3.4.1 Penjelasan tahap lanjutan menentukan ruang lingkup SMKI

1. Mengidentifikasi masalah eksternal dan internal yang relevan dengan tujuan dan yang mempengaruhi kemampuan untuk mencapai hasil yang diharapkan dari sistem manajemen keamanan informasi.
2. Identifikasi kondisi existing organisasi, antara lain: karakteristik proses bisnis yang dimiliki organisasi, lokasi organisasi, aset-aset yang miliki, teknologi yang digunakan.
3. Menetapkan persyaratan pihak yang berkepentingan. Persyaratan ini mencakup komitmen manajemen.



Gambar 3.4.1-1 Alur Ruang Lingkup SMKI

3.4.2 Lanjutan proses Identifikasi risiko

Proses identifikasi risiko ini memiliki empat langkah, yaitu:

a. Langkah 1: Identifikasi aset dan klasifikasi aset dengan menggunakan tabel aset
b. Langkah 2: Menghitung nilai aset berdasarkan aspek keamanan informasi (CIA) dengan memberikan nilai masing-masing, setelah ini dihitung nilai asetnya yaitu dengan menggunakan persamaan matematis berikut:

Nilai Aset (NA)= NC+NI+NV.....(5)

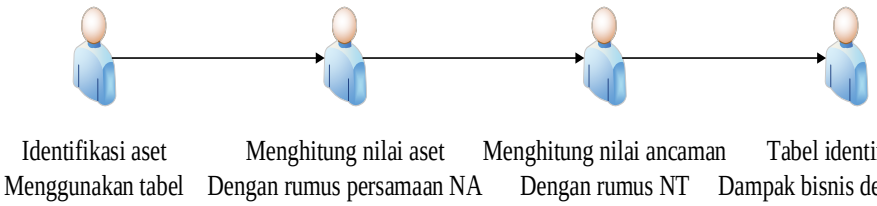
c. Langkah 3: Menghitung nilai ancaman dan kelemahan aset

a. Membuat tabel kemungkinan gangguan

b. Membuat tabel penghitungan nilai ancaman dengan rumus:

Nilai ancaman (NT)= ∑PO / ∑Ancaman.....(6)

d. Langkah 4: Identifikasi dampak kegagalan terhadap aspek keamanan informasi (CIA) yaitu dengan membuat tabel identifikasi dampak bisnis disertai level dampak yang terjadi.



Gambar 3.4.2 Identifikasi Risiko

3.5 Analisa dan evaluasi risiko

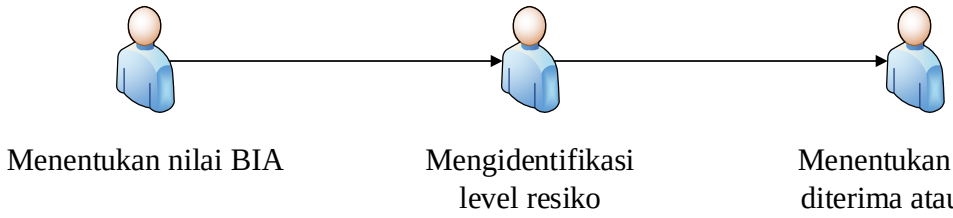
a. Langkah 1: Melakukan Analisa dampak bisnis yang dilakukan dengan cara pembuatan tabel skala nilai *Business Impact Analysis* (BIA), setelah itu dibuat tabel BIA sesuai dengan fasilitas informasi yang dimiliki organisasi dengan mengacu pada tabel nilai skala BIA.

b. Langkah 2: identifikasi level risiko dilakukan dengan membuat tabel matriks level risiko dengan menggunakan nilai probabilitas ancaman dan nilai BIA.

c. Langkah 3: menentukan risiko diterima atau perlunya pengelolaan. Cara menilai risiko dapat dihitung dengan menggunakan metode matematis dengan rumus:

Nilai Risiko (Risk Value) = NA x BIA x NT .....(7)

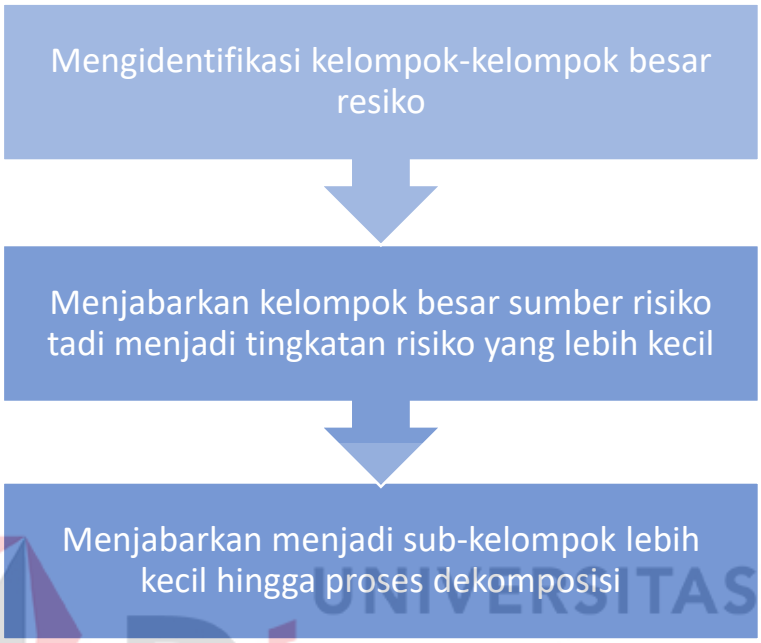
Selanjutnya perlu ditentukan level risikonya dari hasil perhitungan matematis



Gambar 3.5 Analisa dan Evaluasi Risiko

3.7 Lanjutan Tahapan *Risk Breakdown Structure*

Tahapan RBS digambarkan pada Gambar 3.7.



Gambar 3.7 Pendekatan RBS Top-Down

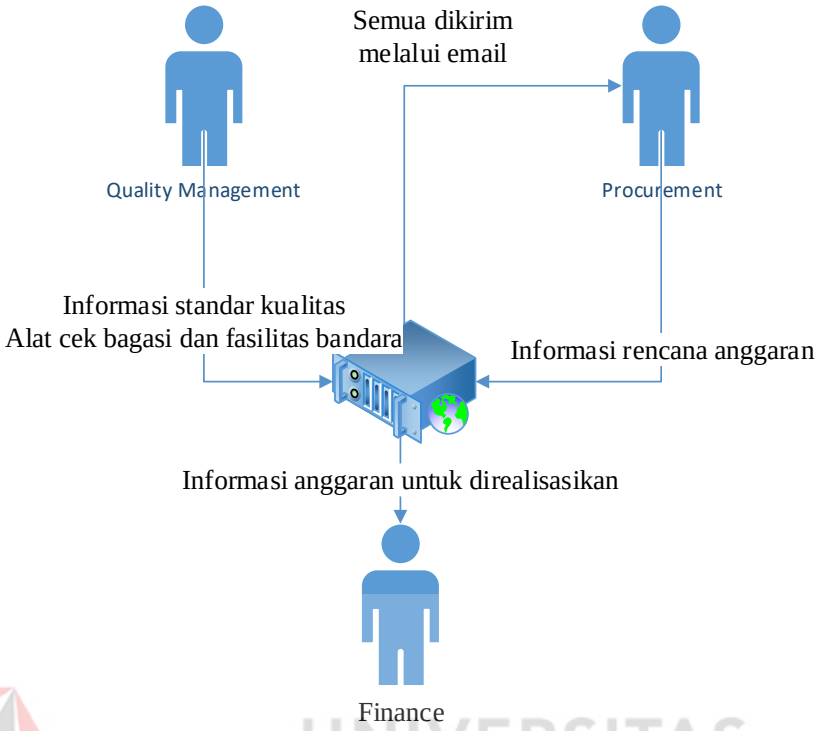
Penjelasan tentang risiko-risiko yang mungkin terjadi dan pengelompokan risiko berdasarkan aspek beserta klausul yang dibutuhkan untuk menyelesaikan masalah dijelaskan pada tabel 3.7.

Tabel 3.7 *Risk Breakdown Structure*

No	Risiko terhadap CIA	Aspek	Permasalahan	Klausul
1	Kehilangan atau kerusakan informasi terkait perencanaan pengadaan alat bagasi	Managerial	Tidak adanya kebijakan keamanan informasi yang dikomunikasikan ke semua staff	Klausul 5
		Teknikal	Belum adanya kebijakan peran dam tanggung jawab keamanan informasi	Klausul 6
		Operasional	Tidak ada aturan tentang keamanan *transfer* informasi	Klausul 12
2	Kehilangan data jadwal penerbangan	Managerial	Tidak adanya kebijakan keamanan informasi yang dikomunikasikan ke semua staff	Klausul 5

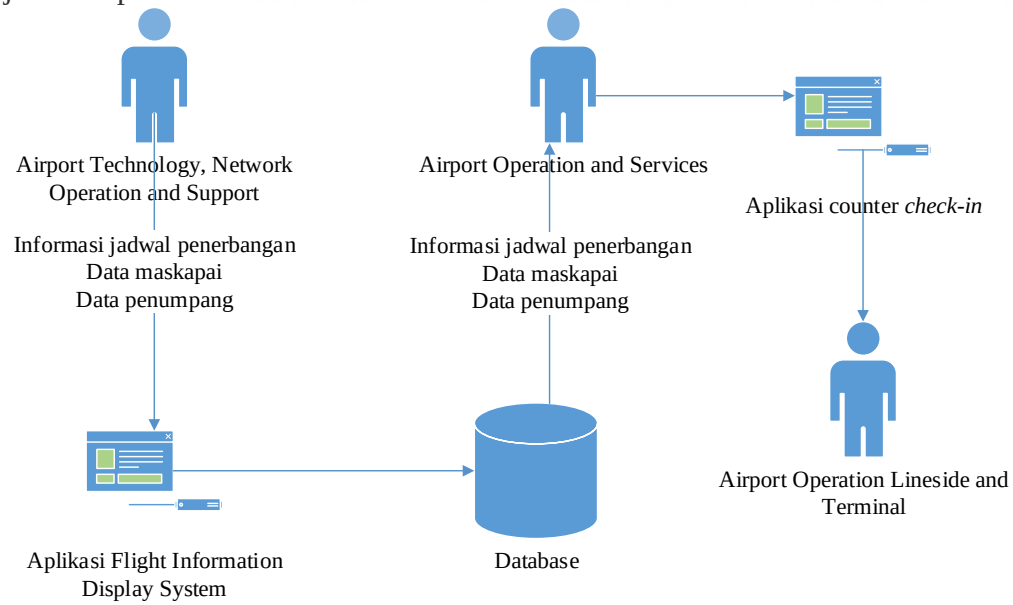
		Teknikal	Belum adanya kebijakan akses kontrol untuk penggunaan aplikasi FIDS, Tidak adanya keamanan terkait ancaman berupa *virus, worm, dan malware.* Kondisi saat ini pernah terjadi kehilangan informasi jadwal penerbangan karena kurangnya kebijakan manajemen insiden	Klausul 9 Klausul 12
		Operasional	Kurangnya kebijakan tentang lingkungan sekitar penyimpanan informasi penting saat *recovery* ketika *server down*	Klausul 11
3	Tidak tersedianya informasi jadwal *shift* kerja pegawai	Managerial	Belum adanya manajemen penerapan keamanan informasi pada organisasi	Klausul 6
		Teknikal	-	
		Operasional	-	
4	Rusak atau hilangnya data maskapai	Managerial	Belum adanya manajemen asset terkait data maskapai	Klausul 8
		Teknikal	Kurangnya kebijakan tentang lingkungan sekitar penyimpanan informasi penting	Klausul 11
		Operasional	-	
5	Tidak tersedianya informasi operator garbarata	Managerial	Belum adanya manajemen penerapan keamanan informasi pada organisasi	Klausul 6
		Teknikal	Belum adanya kebijakan tanggung jawab tiap sumber daya manusianya terkait keamanan informasi	Klausul 7
		Operasional	-	
6	Tidak tersedianya informasi perencanaan pengadaan fasilitas bandara	Managerial	Tidak ada kebijakan keamanan informasi	Klausul 5
		Teknikal	Belum adanya kebijakan hak akses terhadap penggunaan informasi terkait perencanaan pengadaan barang	Klausul 9
		Operasional	-	
7	Hilang atau rusaknya informasi terkait hasil evaluasi tiap layanan bisnis utama	Managerial	Kurangnya kebijakan manajemen aset informasi	Klausul 8
		Teknikal	Ketika transfer data atau informasi hanya melalui email yang	Klausul 5
		Operasional	-	

Alur informasi yang harus dilindungi pada proses pengadaan alat cek bagasi dan fasilitas pengunjung bandara dijelaskan pada Gambar 3.7-2.



Gambar 3.7-2 Alur informasi pada bagian pengadaan alat cek bagasi dan fasilitas bandara

Alur informasi yang harus dilindungi pada proses pengendalian bagasi dijelaskan pada Gambar 3.7-3.



Gambar 3.7-2 Alur Informasi Pengendalian Bagasi

LAMPIRAN 8

LANJUTAN HASIL DAN PEMBAHASAN

4.2.2 poin 1 Identifikasi Aset

Tabel 4.2.2 Aset Organisasi

No.	Kategori Aset	Daftar Aset
1.	Hardware	*X-Ray, WMTD, Body Scanner*
		Hand Held
		Access Door
		CCTV
		Radio Trucking
		WIFI
		Telephone
		PC
		Server
		Printer
		Fire alarm
2.	*Software*	Aplikasi FIDS
		Aplikasi *Counter check-in*
3.	Jaringan	WIFI
		Router
		Switch
		SAP (Layanan VPN)
		POSS (Layanan Internet)
		Kabel
4.	Data	Data *center*
		Data Jadwal Penerbangan
		Data Jadwal Shift Kerja pegawai
		Data Maskapai
		Data Perencanaan Pengadaan fasilitas bandara

		Data Pengendalian Bagasi
		Data Operator Garbarata
		Data hasil evaluasi tiap layanan bisnis utama
		Data Keuangan
		Data Calon Penumpang
		Data Aset
5.	Sumber Daya Manusia/SDM	Pegawai
		Satuan Pengamanan

Dari hasil observasi dianalisa Kembali dalam menghasilkan asset informasi kritis yang digunakan dalam proses penelitian selanjutnya

4.2.2 poin 3 Lanjutan Tabel Aset Kritis

Tabel 4.2.2-3 – Daftar Aset Kritis

No.	Kategori Aset	Daftar Aset	Alasan/Sebab
1.	*Hardware*	*Server*	Server bertujuan untuk memastikan data dan sistem selalu dapat diakses setiap saat
		PC	Komputer juga digunakan untuk proses operasional dan juga sebagai media untuk mengakses data PC
2.	*Software*	FIDS	*Flight Information Display System* (FIDS) bertujuan memberikan informasi terkait jadwal penerbangan, data maskapai, data bagasi, data penumpang, dan data operator garbarata.
		Counter check-in	Aplikasi *counter check-in* bertujuan untuk membantu calon penumpang ketika *check-in.*
3.	Jaringan	WIFI	Jaringan digunakan untuk mengakses informasi, seperti mengakses *database* dan mengakses *internet*
		Router	
		Switch	
		Kabel	
		POSS (Layanan Internet)	

Tabel 4.2.2-3 (Lanjutan)

No.	Kategori Aset	Daftar Aset	Alasan/Sebab
		SAP (Layanan VPN)	
4.	Data	Data *center*	Seluruh data sangat penting bagi instansi karena terkait dengan keberlangsungan proses bisnis instansi sehingga keamanan dari setiap data sangat penting
		Data jadwal penerbangan	
		Data shift kerja pegawai	
		Data maskapai	
		Data perencanaan pengadaan fasilitas bandara	
		Data Pengendalian Bagasi	
		Data operator garbarata	
		Data keuangan	
		Data hasil evaluasi tiap layanan bisnis utama	
		Data aset	
		Data calon penumpang	
5.	Sumber Daya Manusia/SDM	Pegawai	Suatu aset yang penting dalam sebuah organisasi karena SDM yang memiliki kompetensi dapat mendukung proses bisnis berjalan dengan lancar.
		Satuan Pengamanan	

4.2.2 poin 5 Lanjutan tabel identifikasi kerentanan

Tabel 4.2.2-5 – Identifikasi kerentanan

Server	
System of Interest	*Server* pada instansi
Komponen Utama	Kemungkinan Ancaman

• Sistem Operasi • *Processor* • RAM • *Harddisk* • Listrik • Keamanan Jaringan • *Genset* • UPS • Kabel • Pendingin ruangan • Ruang *Server*	• Tidak mendapatkan aliran listrik karena terjadi pemadaman listrik • Genset tidak dapat berfungsi karena mengalami kerusakan • RAM mengalami kelebihan memori • Kinerja Processor menurun akibat terlalu banyak kapasitas data • Tempat penyimpanan (*Harddisk*) penuh • Keamanan jaringan dapat ditembus • Kerusakan infrastruktur jaringan • UPS tidak berfungsi • Komponen dicuri karena kelalaian pihak keamanan
PC	
System of Interest	PC yang ada pada instansi
Komponen Utama	Kemungkinan Ancaman
• CPU • Monitor, Keyboard dan Mouse • Kabel LAN • *Antivirus* • Sistem Operasi • *Software* • Listrik • UPS • *Genset* • *Firewall*	• *Monitor*, *Keyboard* ataupun *mouse* mengalami kerusakan • *Firewall* ditembus oleh bagian yang tidak berwenang • Kabel LAN putus akibat hewan pengerat • Tidak mendapatkan aliran listrik karena terjadi pemadaman pada PLN • UPS tidak berfungsi • Virus yang menyerang tidak dapat tertangani oleh antivirus • Komponen di curi karena kelalaian pihak keamanan
Data	
System of Interest	Seluruh data yang dimiliki instansi
Komponen Utama	Kemungkinan Ancaman

• *Database* • *Server* • Listrik • PC • *Firewall* • *Data center*	• Tidak dapat mendapatkan aliran listrik karena terjadi pemadaman pada PLN • *Firewall* ditembus oleh bagian yang tidak berwenang • PC berhenti beroperasi karena terserang virus • Data dicuri karena kurangnya manajemen keamanan informasi
Perangkat Lunak	
System of Interest	*Flight information display System* (FIDS), aplikasi counter *check-in*
Komponen Utama	Kemungkinan Ancaman
• *Firewall* • *Server* • *Antivirus*	• *Firewall* ditembus oleh bagian yang tidak berwenang • *Virus* yang menyerang tidak dapat tertangani oleh *antivirus* • *Server* mengalami kerusakan sehingga sistem tidak dapat diakses
WIFI	
System of Interest	WIFI yang terpasang semua berada dalam 1 kantor
Komponen Utama	Kemungkinan Ancaman
• Listrik • Kabel • Keamanan Jaringan	• Tidak mendapatkan aliran listrik karena terjadi pemadaman • Kabel rusak akibat gigitan hewan • Keamanan jaringan dapat ditembus oleh pihak yang tidak berwenang • Kerusakan infrastruktur jaringan
Router	
System of Interest	4 Router pada ICT
Komponen Utama	Kemungkinan Ancaman

• Listrik • Kabel • Keamanan Jaringan	• Tidak mendapatkan aliran listrik karena terjadi pemadaman • Kabel rusak akibat digigit hewan pengerat • Komponen dicuri karena kelalaian pihak keamanan • Kerusakan infrastruktur jaringan

Lanjutan 4.4 Tabel menghitung aset kritis

Dari hasil wawancara dan observasi yang dilakukan diperoleh nilai masing – masing aset pada ICT yang dapat dilihat pada tabel 4.6

Tabel 4.4– Nilai Aset ICT

No	Kategori Aset	Daftar Aset	Kriteria			Nilai Aset (NC+NI+NV)
			Nilai *Confidentiality* (NC)	Nilai *Integrity* (NI)	Nilai *Availability* (NV)	
1.	*Hardware*	*Server*	4	4	3	11
		PC	3	3	3	9
2.	*Software*	*Flight Information Display System* (FIDS)	4	4	4	12
		Aplikasi *counter check-in*	4	4	4	12
3.	Jaringan	Wifi	2	2	3	7
		Router dan Switch	3	3	3	9
		Kabel	2	3	3	8
		Data *center*	4	4	4	12
		Data jadwal penerbangan	4	4	4	12

4.	Data	Data jadwal shift kerja pegawai	3	3	3	9
		Data Keuangan	4	4	4	12
		Data maskapai	4	4	4	12
		Data calon penumpang	4	4	4	12
		Data pengendalian bagasi	4	4	4	12
		Data operator garbarata	4	4	3	11
		Data maskapai	4	4	3	11

		Data evaluasi layanan bisnis utama	4	4	4	12
		Data perencanaan pengadaan fasilitas bandara	4	4	4	12
		Data Aset	3	3	3	9
5.	SDM	Pegawai	4	3	3	10
		Satuan Pengamanan	3	3	3	9

4.4.2 Tabel lanjutan menentukan kemungkinan (*Probability*)

Penilaian identifikasi ancaman, kelemahan, dan *probability* dapat dilihat pada tabel 4.4.2-1

Tabel 4.4.2-1 - Penilaian ancaman, kelemahan, dan probabilitas pada *Server*

Nama Aset	Server		
Jenis Aset	Hardware		
Risiko	Jenis Kejadian	*Probability*	Rata-rata *Probability*
Bencana alam	*Threat*	*Low*	0,2
Kehilangan data	*Vulnerable*	*Low*	0,2
Kerusakan server	*Threat*	*Medium*	0,4
Pencurian komponen Server	*Threat*	*Medium*	0,6
Kesalahan konfigurasi Server	*Vulnerable*	*Medium*	0,4
Akses *ilegal*	*Threat*	*Medium*	0,4
Server mati/down	*Threat*	*Low*	0,2
Serangan virus	*Vulnerable*	*High*	0,8
Jumlah Ancaman = 8	Jumlah rata-rata *probabilitas*		3,2
Nilai *Threat* (NT)	Jumlah rata-rata *probabilitas* / Jumlah ancaman 3,2 / 8 = 0,4		

Identifikasi pada aset *Server* memiliki 8 ancaman, dengan jumlah rata-rata *probabilitasnya* 3,2 dan nilai ancamannya adalah 0,4. Identifikasi ancaman, kelemahan, dan *probabilitas* pada PC dapat dilihat pada Tabel 4.4.2-2

Tabel 4.4.2-2 - Penilaian ancaman, kelemahan, dan *probabilitas* pada PC

Nama Aset	PC		
Jenis Aset	*Hardware*		
Risiko	Jenis Kejadian	*Probability*	Rata-rata *Probability*
Bencana alam	*Threat*	*Low*	0,2
PC rusak	*Threat*	*Medium*	0,4
Kehilangan data	*Threat*	*High*	0,8
Kerusakan komponen PC	*Vulnerable*	*Low*	0,2
Pencurian komponen *Hardware*	*Vulnerable*	*Low*	0,2
Akses ilegal	*Threat*	*High*	0,8
Kesalahan konfigurasi *Hardware*	*Vulnerable*	*High*	0,8
Jumlah ancaman = 7	Jumlah rata-rata *probabilitas*		3,4
Nilai *Threat* (NT)	Jumlah rata-rata *probabilitas* / Jumlah ancaman 3,4 /7 = 0,48		

Identifikasi pada aset PC memiliki 7 ancaman, dengan jumlah rata-rata probabilitasnya 3,4 dan nilai ancamannya adalah 0,48. Identifikasi ancaman, kelemahan, dan *probabilitas* pada *flight Information display system* (FIDS) (software) dapat dilihat pada Tabel 4.4.2-3

Tabel 4.4.2-3 - Penilaian ancaman, kelemahan, dan *probabilitas* pada FIDS

Nama Aset	*Flight Information Display system* (FIDS)		
Jenis Aset	*Software*		
Risiko	Jenis Kejadian	*Probability*	Rata-rata *Probability*
Bug pada aplikasi/sistem tidak berjalan dengan normal	*Vulnerable*	*Medium*	0,2

Serangan *virus*, *worm*, dan *malware*	*Threat*	*High*	1,0
Kesalahan konfigurasi dan input data pada sistem	*Vulnerable*	*Low*	0,2
Pembobolan sistem/akses ilegal	*Threat*	*High*	1,0
Kehilangan data	*Threat*	*Medium*	0,4
Sistem tidak dapat Diakses	*Vulnerable*	*Low*	0,2
Jumlah ancaman = 6	Jumlah rata-rata *probabilitas*		3,0
Nilai *Threat* (NT)	Jumlah rata-rata *probabilitas* / Jumlah ancaman 3,0 /6 = 0,5		

Identifikasi pada *Flight Information Display system* (FIDS) memiliki 6 ancaman, dengan jumlah rata-rata probabilitasnya 3,0 dan nilai ancamannya adalah 0,5. Identifikasi ancaman, kelemahan, dan probabilitas pada aplikasi *counter check-in (software)* dapat dilihat pada Tabel 4.4.2-4

Tabel 4.4.2-4 - Penilaian ancaman, kelemahan, dan *probabilitas* pada *counter check-in*

Nama Aset	Aplikasi *counter check-in*		
Jenis Aset	*Software*		
Risiko	Jenis Kejadian	*Probability*	Rata-rata *Probability*
Bug pada aplikasi/sistem tidak berjalan dengan Normal	*Vulnerable*	*Low*	0,2
Serangan *virus*, *worm*, dan *malware*	*Threat*	*high*	0,8
Kesalahan konfigurasi dan input data pada sistem	*Vulnerable*	*Low*	0,2
Pembobolan sistem/akses ilegal	*Threat*	*High*	1,0
Kehilangan data	*Threat*	*Low*	0,2

Sistem tidak dapat Diakses	*Vulnerable*	*Low*	0,2
Jumlah ancaman = 6	Jumlah rata-rata *probabilitas*		2,6
Nilai *Threat* (NT)	Jumlah rata-rata *probabilitas* / Jumlah ancaman 2,6 /6 = 0,43		

Identifikasi pada aset Aplikasi *counter check-in* memiliki 6 ancaman, dengan jumlah rata-rata probabilitasnya 2,6 dan nilai ancamannya adalah 0,43. Identifikasi ancaman kelemahan, dan *probabilitas* pada wifi (jaringan) dapat dilihat pada Tabel 4.4.2-5

Tabel 4.4.2-5 - Penilaian ancaman, kelemahan, dan *probabilitas* pada WIFI

Nama Aset	Wifi		
Jenis Aset	Jaringan		
Risiko	Jenis Kejadian	*Probability*	Rata-rata *Probability*
Akses ilegal	*Threat*	*High*	0,8
Monopoly bandwidth	*Vulnerable*	*High*	0,8
Serangan virus	*Threat*	*High*	0,6
Kerusakan hardware	*Vulnerable*	*Medium*	0,4
Gangguan wifi	*Vulnerable*	*Low*	0,2
Hilangnya komponen *Hardware*	*Vulnerable*	*Low*	0,2
Pembobolan jaringan	*Threat*	*High*	0,8
Jumlah ancaman = 7	Jumlah rata-rata *probabilitas*		3,8
Nilai *Threat* (NT)	Jumlah rata-rata *probabilitas* / Jumlah ancaman 3,8 /7 = 0,54		

Identifikasi pada aset Wifi memiliki 7 ancaman, dengan jumlah rata-rata probabilitasnya 3,8 dan nilai ancamannya adalah 0,54. Identifikasi ancaman, kelemahan, dan *probabilitas* pada *Router* dan *Switch* (jaringan) dapat dilihat pada Tabel 4.4.2-6

Tabel 4.4.2-6 - Penilaian ancaman, kelemahan, dan probabilitas pada *Router Switch*

Nama Aset	*Router* dan *Switch*		
Jenis Aset	Jaringan		
Risiko	Jenis Kejadian	*Probability*	Rata-rata *Probability*
Akses illegal	*Threat*	*High*	0,8
Monopoly bandwidth	*Vulnerable*	*High*	0,8
Serangan virus	*Threat*	*Medium*	0,6
Kerusakan *hardware*	*Vulnerable*	*Low*	0,2
Gangguan router	*Vulnerable*	*Low*	0,2
Hilangnya komponen Hardware	*Vulnerable*	*Low*	0,2
Pembobolan jaringan	*Threat*	*High*	0,8
Jumlah ancaman = 7	Jumlah rata-rata *probabilitas*		3,6
Nilai *Threat* (NT)	Jumlah rata-rata *probabilitas* / Jumlah ancaman 3,6 /7 = 0,51		

Identifikasi pada aset *Router* dan *Switch* memiliki 7 ancaman, dengan jumlah rata-rata probabilitasnya 4,0 dan nilai ancamannya adalah 0,57. Identifikasi ancaman, kelemahan, dan *probabilitas* pada kabel (jaringan) dapat dilihat pada Tabel 4.4.2-7.

Tabel 4.4.2-7 - Penilaian ancaman, kelemahan, dan *probabilitas* pada kabel jaringan

Nama Aset	Kabel		
Jenis Aset	Jaringan		
Risiko	Jenis Kejadian	*Probability*	Rata-rata *Probability*
Kerusakan *hardware*	*Vulnerable*	*Medium*	0,4
Gangguan kabel	*Vulnerable*	*Medium*	0,4
Hilangnya komponen	*Vulnerable*	*Low*	0,2
Jumlah ancaman = 3	Jumlah rata-rata *probabilitas*		1,0
Nilai *Threat* (NT)	Jumlah rata-rata *probabilitas* / Jumlah ancaman 1,0 /3 = 0,33		

Identifikasi pada asset Kabel memiliki 3 ancaman, dengan jumlah rata-rata probabilitasnya 1,0 dan nilai ancamannya adalah 0,33. Identifikasi ancaman, kelemahan, dan *probabilitas* pada Data *center* (data) dapat dilihat pada Tabel 4.4.2-7

Tabel 4.4.2-7 - Penilaian ancaman, kelemahan, dan *probabilitas* pada data *center*

Nama Aset	Data *Center*		
Jenis Aset	Data		
Risiko	Jenis Kejadian	*Probability*	Rata-rata *Probability*
Kesalahan input data	*Vulnerable*	*Medium*	0,4
Manipulasi data	*Threat*	*High*	0,8
Data hilang	*Threat*	*Medium*	0,4
Pencurian data	*Threat*	*High*	0,8
Data tidak dapat Diakses	*Vulnerable*	*Medium*	0,4
Data *corrupt*/rusak	*Vulnerable*	*Low*	0,2
Serangan virus	*Threat*	*High*	0,8
Akses *ilegal*	*Threat*	*High*	1,0
Jumlah ancaman = 8	Jumlah rata-rata *probabilitas*		3,8
Nilai *Threat* (NT)	Jumlah rata-rata *probabilitas* / Jumlah ancaman 3,8 /8 = 0,48		

Identifikasi pada Data *Center* memiliki 8 ancaman, dengan jumlah rata-rata probabilitasnya 0,48 dan nilai ancamannya adalah 0,48. Identifikasi ancaman, kelemahan, dan probabilitas pada Data Jadwal Penerbangan dapat dilihat pada Tabel 4.4.2-8

Tabel 4.4.2-8 - Penilaian ancaman, kelemahan, dan probabilitas pada Data Jadwal Penerbangan

Nama Aset	Data Jadwal Penerbangan		
Jenis Aset	Data		
Risiko	Jenis Kejadian	*Probability*	Rata-rata *Probability*

Kesalahan input data	*Vulnerable*	*Low*	0,2
Manipulasi data	*Threat*	*Low*	0,2
Data hilang	*Threat*	*Medium*	0,4
Pencurian data	*Threat*	*Medium*	0,6
Data tidak dapa Diakses	*Vulnerable*	*Low*	0,2
Data *corrupt*/rusak	*Vulnerable*	*Low*	0,2
Serangan virus	*Threat*	*Medium*	0,6
Akses *ilegal*	*Threat*	*High*	1,0
Jumlah ancaman = 8	Jumlah rata-rata probabilitas		3,4
Nilai Threat (NT)	Jumlah rata-rata probabilitas / Jumlah ancaman 3,4 /8 = 0.43		

Identifikasi pada data jadwal penerbangan memiliki 8 ancaman, dengan jumlah rata-rata probabilitasnya 3,4 dan nilai ancamannya adalah 0,43. Identifikasi ancaman, kelemahan, dan probabilitas pada Data Jadwal Shift Kerja Pegawai dapat dilihat pada Tabel 4.4.2-9

Tabel 4.4.2-9 - Penilaian ancaman, kelemahan, dan probabilitas pada Data Jadwal Shift Kerja Pegawai

Nama Aset	Data Jadwal Shift Kerja Pegawai		
Jenis Aset	Data		
Risiko	Jenis Kejadian	*Probability*	Rata-rata *Probability*
Kesalahan input data	*Vulnerable*	*Low*	0,2
Manipulasi data	*Threat*	*Low*	0,2
Data hilang	*Threat*	*Medium*	0,4
Pencurian data	*Threat*	*Medium*	0,4
Data tidak dapat Diakses	*Vulnerable*	*Medium*	0,4
Data *corrupt*/rusak	*Vulnerable*	*Medium*	0,4
Serangan virus	*Threat*	*Medium*	0,4
Akses illegal	*Threat*	*High*	0,8
Jumlah ancaman = 8	Jumlah rata-rata probabilitas		4,9

Nilai *Threat* (NT)	Jumlah rata-rata probabilitas / Jumlah ancaman 3,2 /8 = 0,4

Identifikasi pada Data Jadwal Shift Kerja Pegawai memiliki 8 ancaman, dengan jumlah rata-rata probabilitasnya 3,2 dan nilai ancamannya adalah 0,4. Identifikasi ancaman, kelemahan, dan probabilitas pada Data Keuangan (data) dapat dilihat pada Tabel 4.4.2-10

Tabel 4.4.2-10 - Penilaian ancaman, kelemahan, dan probabilitas pada data keuangan

Nama Aset	Data Keuangan		
Jenis Aset	Data		
Risiko	Jenis Kejadian	*Probability*	Rata-rata *Probability*
Kesalahan input data	*Vulnerable*	*Low*	0,2
Manipulasi data	*Threat*	*Medium*	0,4
Data hilang	*Threat*	*Low*	0,2
Pencurian data	*Threat*	*Medium*	0,4
Data tidak dapat Diakses	*Vulnerable*	*Low*	0,2
Data *corrupt*/rusak	*Vulnerable*	*High*	0,2
Serangan virus	*Threat*	*Medium*	0,6
Akses illegal	*Threat*	*High*	1,0
Jumlah ancaman = 8	Jumlah rata-rata probabilitas		3,2
Nilai *Threat* (NT)	Jumlah rata-rata probabilitas / Jumlah ancaman 3,2 /8 = 0,4		

Identifikasi pada Data Keuangan memiliki 8 ancaman, dengan jumlah rata-rata probabilitasnya 3,2 dan nilai ancamannya adalah 0,4. Identifikasi ancaman, kelemahan, dan probabilitas pada Data Perencanaan pengadaan fasilitas bandara dapat dilihat pada Tabel 4.4.2-11

Tabel 4.4.2-11 - Penilaian ancaman, kelemahan, dan probabilitas pada Data Perencanaan pengadaan fasilitas bandara

Nama Aset	Perencanaan pengadaan fasilitas bandara		
Jenis Aset	Data		
Risiko	Jenis Kejadian	*Probability*	Rata-rata *Probability*
Kesalahan input data	*Vulnerable*	*Low*	0,2
Manipulasi data	*Threat*	*Medium*	0,6
Data hilang	*Threat*	*Low*	0,2
Pencurian data	*Threat*	*Medium*	0,4
Data tidak dapat diakses	*Vulnerable*	*Low*	0,2
Data *corrupt*/rusak	*Vulnerable*	*Low*	0,2
Serangan virus	*Threat*	*Medium*	0,4
Akses illegal	*Threat*	*Medium*	0,6
Jumlah ancaman = 8	Jumlah rata-rata probabilitas		2,8
Nilai *Threat* (NT)	Jumlah rata-rata probabilitas / Jumlah ancaman 2,8 /8 = 0,35		

Identifikasi pada data Perencanaan pengadaan fasilitas bandara memiliki 8 ancaman, dengan jumlah rata-rata probabilitasnya 2,8 dan nilai ancamannya adalah 0,35. Identifikasi ancaman, kelemahan, dan probabilitas pada Data aset (data) dapat dilihat pada Tabel 4.4.2-12

Tabel 4.4.2-12 - Penilaian ancaman, kelemahan, dan probabilitas pada Data Aset

Nama Aset	Data Aset		
Jenis Aset	Data		
Risiko	Jenis Kejadian	Probability	Rata-rata Probability
Kesalahan input data	*Vulnerable*	*Medium*	0,4
Manipulasi data	*Threat*	*Low*	0,2
Data hilang	*Threat*	*Low*	0,2
Pencurian data	*Threat*	*Medium*	0,6
Data tidak dapat Diakses	*Vulnerable*	*Medium*	0,4
Data *corrupt*/rusak	*Vulnerable*	*Low*	0,2

Serangan virus	*Threat*	*High*	0,8
Akses illegal	*Threat*	*High*	0,8
Jumlah ancaman = 8	Jumlah rata-rata probabilitas		3,6
Nilai *Threat* (NT)	Jumlah rata-rata probabilitas / Jumlah ancaman 3,6 /8 = 0,45		

Identifikasi pada Data aset sistem informasi presensi memiliki 8 ancaman, dengan jumlah rata-rata probabilitasnya 3,6 dan nilai ancamannya adalah 0,45.

Identifikasi ancaman, kelemahan, dan probabilitas pada Data evaluasi tiap layanan bisnis utama dapat dilihat pada Tabel 4.4.2-13

Tabel 4.4.2-13 - Penilaian ancaman, kelemahan, dan probabilitas pada Data Evaluasi tiap layanan bisnis utama

Nama Aset	Evaluasi tiap layanan bisnis utama		
Jenis Aset	Data		
Risiko	Jenis Kejadian	Probability	Rata-rata Probability
Kesalahan input data	*Vulnerable*	*Low*	0,2
Manipulasi data	*Threat*	*Low*	0,2
Data hilang	*Threat*	*Low*	0.2
Pencurian data	*Threat*	*Medium*	0,4
Data tidak dapat Diakses	*Vulnerable*	*Low*	0,2
Data *corrupt*/rusak	*Vulnerable*	*Low*	0,2
Serangan virus	*Threat*	*High*	0,8
Akses illegal	*Threat*	*High*	0,8
Jumlah ancaman = 8	Jumlah rata-rata probabilitas		3,0
Nilai Threat (NT)	Jumlah rata-rata probabilitas / Jumlah ancaman 3 /8 = 0,37		

Identifikasi pada data evaluasi tiap layanan bisnis utama memiliki 8 ancaman, dengan jumlah rata-rata probabilitasnya 3 dan nilai ancamannya adalah

0,37.

Identifikasi ancaman, kelemahan, dan probabilitas pada operator garbarata dapat dilihat pada Tabel 4.4.2-14

Tabel 4.4.2-14 - Penilaian ancaman, kelemahan, dan probabilitas pada Data operator garbarata

Nama Aset	Data operator garbarata		
Jenis Aset	Data		
Risiko	*Jenis Kejadian*	*Probability*	Rata-rata *Probability*
Kesalahan input data	*Vulnerable*	*Low*	0,2
Manipulasi data	*Threat*	*Low*	0,2
Data hilang	*Threat*	*Low*	0,2
Pencurian data	*Threat*	*Medium*	0,4
Data tidak dapat Diakses	*Vulnerable*	*Low*	0,2
Data *corrupt*/rusak	*Vulnerable*	*Low*	0,2
Serangan virus	*Threat*	*Medium*	0,6
Akses illegal	*Threat*	*High*	1,0
Jumlah ancaman = 8	Jumlah rata-rata probabilitas		3,0
Nilai *Threat* (NT)	Jumlah rata-rata probabilitas / Jumlah ancaman 3,0 /8 = 0,38		

Identifikasi pada data operator garbarata memiliki 8 ancaman, dengan jumlah rata-rata probabilitasnya 3,0 dan nilai ancamannya adalah 0,38 Identifikasi ancaman, kelemahan, dan probabilitas pada data pengendalian bagasi dapat dilihat pada Tabel 4.4.2-15

Tabel 4.4.2-15 - Penilaian ancaman, kelemahan, dan probabilitas pada Data Pengendalian bagasi

Nama Aset	Data pengendalian bagasi		
Jenis Aset	Data		
Risiko	Jenis Kejadian	*Probability*	Rata-rata *Probability*
Kesalahan input data	*Vulnerable*	*Low*	0,4

Manipulasi data	*Threat*	*Low*	0,4
Data hilang	*Threat*	*Medium*	0,4
Pencurian data	*Threat*	*Medium*	0,6
Data tidak dapat Diakses	*Vulnerable*	*Low*	0,2
Data corrupt/rusak	*Vulnerable*	*Medium*	0,4
Serangan virus	*Threat*	*High*	0,8
Akses ilegal	*Threat*	*High*	1,0
Jumlah ancaman = 8	Jumlah rata-rata probabilitas		4,2
Nilai *Threat* (NT)	Jumlah rata-rata probabilitas / Jumlah ancaman 4,2 /8 = 0,53		

Identifikasi pada data pengendalian bagasi memiliki 8 ancaman, dengan jumlah rata-rata probabilitasnya 4,2 dan nilai ancamannya adalah 0,53.

Identifikasi ancaman, kelemahan, dan probabilitas pada data maskapai dapat dilihat pada Tabel 4.4.2-16

Tabel 4.4.2-16 - Penilaian ancaman, kelemahan, dan probabilitas pada Data maskapai

Nama Aset	Data maskapai		
Jenis Aset	Data		
Risiko	Jenis Kejadian	*Probability*	Rata-rata *Probability*
Kesalahan input data	*Vulnerable*	*Low*	0,2
Manipulasi data	*Threat*	*Low*	0,2
Data hilang	*Threat*	*Medium*	0,4
Pencurian data	*Threat*	*Medium*	0,4
Data tidak dapat Diakses	*Vulnerable*	*Low*	0,2
Data *corrupt*/rusak	*Vulnerable*	*Medium*	0,4
Serangan virus	*Threat*	*High*	0,8
Akses ilegal	*Threat*	*High*	1,0
Jumlah ancaman = 8	Jumlah rata-rata probabilitas		3,6

Nilai *Threat* (NT)	Jumlah rata-rata probabilitas / Jumlah ancaman 3,6 /8 = 0,45

Identifikasi pada data maskapai memiliki 8 ancaman, dengan jumlah rata-rata probabilitasnya 3,6 dan nilai ancamannya adalah 0,45.

Identifikasi ancaman, kelemahan, dan probabilitas pada data calon penumpang dapat dilihat pada Tabel 4.4.2-17

Tabel 4.4.2-17 - Penilaian ancaman, kelemahan, dan probabilitas pada Data calon penumpang

Nama Aset	Data calon penumpang		
Jenis Aset	Data		
Risiko	Jenis Kejadian	*Probability*	Rata-rata *Probability*
Kesalahan input data	*Vulnerable*	*Low*	0,2
Manipulasi data	*Threat*	*Low*	0,2
Data hilang	*Threat*	*Low*	0,2
Pencurian data	*Threat*	*Medium*	0,4
Data tidak dapat Diakses	*Vulnerable*	*Medium*	0,4
Data *corrupt*/rusak	*Vulnerable*	*Low*	0,2
Serangan virus	*Threat*	*High*	0,8
Akses ilegal	*Threat*	*High*	1,0
Jumlah ancaman = 8	Jumlah rata-rata probabilitas		3,4
Nilai *Threat* (NT)	Jumlah rata-rata probabilitas / Jumlah ancaman 3,4 /8 = 0,43		

Identifikasi pada data calon penumpang memiliki 8 ancaman, dengan jumlah rata-rata probabilitasnya 3,4 dan nilai ancamannya adalah 0,43.

Identifikasi ancaman, kelemahan, dan probabilitas pada data pegawai (SDM) dapat dilihat pada Tabel 4.4.2-18

Tabel 4.4.2-18 - Penilaian ancaman, kelemahan, dan probabilitas pada data pegawai (SDM)

Nama Aset	Pegawai		
Jenis Aset	SDM		
Risiko	Jenis Kejadian	*Probability*	Rata-rata *Probability*
Penyalahgunaan data Organisasi	*Vulnerable*	*Low*	0,2
Penyalahgunaan hak akses	*Threat*	*Low*	0,2
Data tidak sesuai	*Vulnerable*	*Medium*	0,4
Password shared	*Threat*	*Medium*	0,6
Jumlah ancaman = 4	Jumlah rata-rata probabilitas		1,4
Nilai *Threat* (NT)	Jumlah rata-rata probabilitas / Jumlah ancaman 1,4 /4 = 0,35		

Identifikasi pada aset pegawai (SDM) memiliki 4 ancaman, dengan jumlah rata-rata probabilitasnya 1,4 dan nilai ancamannya adalah 0,35. Identifikasi ancaman, kelemahan, dan probabilitas pada Satuan pengamanan (SDM) dapat dilihat pada Tabel 4.4.2-20

Tabel 4.4.2-20 - Penilaian ancaman, kelemahan, dan probabilitas Satuan pengamanan

Nama Aset	Satuan Pengamanan		
Jenis Aset	Data		
Risiko	Jenis Kejadian	*Probability*	Rata-rata *Probability*
Tidak melakukan monitoring keamanan	Threat	Low	0,2
Jumlah ancaman = 1	Jumlah rata-rata probabilitas		0,2
Nilai Threat (NT)	Jumlah rata-rata probabilitas / Jumlah ancaman 0,2 /1 = 0,2		

Identifikasi pada aset Satuan Pengamanan (SDM) memiliki 1 ancaman, dengan jumlah rata-rata probabilitasnya 0,2 dan nilai ancamannya adalah 0,2.

Hasil penilaian identifikasi ancaman, kelemahan, dan probabilitas pada masing- masing aset dapat dilihat pada tabel 4.4.2-21 – rekap nilai ancaman

masing-masing aset.

Tabel 4.4.2-21 - Rekap nilai ancaman aset

No.	Kategori Aset	Daftar Aset	Nilai Ancaman
1.	Hardware	Server	0,4
		PC	0,48
2.	Software	*Flight Information Display System* (FIDS)	0,5
		Aplikasi Counter *check-in*	0,43
3.	Jaringan	Wifi	0,54
		Router dan Switch	0,51
		Kabel	0,57
4.	Data	Data *center*	0,48
		Data jadwal penerbangan	0,43
		Data jadwal shift kerja pegawai	0,4
		Data maskapai	0,45
		Data perencanaan pengadaan fasilitas bandara	0,35
		Data pengendalian bagasi	0,53
		Data operator garbarata	0,38
		Data hasil evaluasi tiap layanan bisnis utama	0,37
		Data asset	0,45
		Data keuangan	0,4
		Data calon penumpang	0,43
5.	SDM	Pegawai	0,35
		Satuan Pengamanan	0,2

4.4.3 Lanjutan tabel dampak jika terjadi kegagalan

Tabel 4.4.3-1 - Identifikasi dampak server

Kategori	Dampak
Confidentiality/ Kerahasiaan	Jika data server tidak memiliki access control, maka menimbulkan dampak kerugian finansial yang sangat besar bagi internal akibat pencurian data dan kehilangan data yang terdapat pada server disalahgunakan oleh pihak yang tidak bertanggung jawab.
Integrity/ Keutuhan	Jika server mengalami kerusakan, maka semua data yang terdapat didalam Server dapat menjadi corrupt bahkan hilang akibatnya informasi yang dihasilkan tidak utuh dan valid.
Availability/ Ketersediaan	Data dan informasi yang disediakan oleh server harus selalu tersedia kapanpun ketika diakses oleh pengguna karena apabila data tersebut tidak dapat diakses mengganggu kelancaran proses bisnis bagi organisasi akibatnya aplikasi core business tidak dapat diakses oleh semua organisasi.

a. Dampak keamanan informasi PC ditunjukkan pada Tabel 4.4.3-2

Tabel 4.4.3-2 - Identifikasi dampak PC

Kategori	Dampak
Confidentiality/ Kerahasiaan	Jika dat yang terdapat pada PC diakses tanpa izin dapat menyebabkan kerugian seperti kehilangan data utama, perubahan informasi yang diakses secara ilegal, dan kerahasiaan dari data-data utama dapat diketahui oleh pihak lain yang tidak bertanggung jawab dapat menggunakan dan memberikan kerugian bagi individu yang bersangkutan.
Integrity/ Keutuhan	Jika PC mengalami kerusakan atau terkena virus, data dan informasi yang ada di dalam PC dapat rusak (*corrupt*) akibatnya informasi yang ada di dalam PC mejadi tidak utuh dan akurat.
Availability/ Ketersediaan	Jika PC tidak dapat mengotorifikasi hak akses dari pemilik PC, maka pengguna (pemilik PC) tidak dapat mengakses data dan informasi yang berada pada PC.

b. Dampak keamanan *Flight Information Display System* (FIDS) ditunjukkan pada Tabel 4.4.3-3

Tabel 4.4.3-3 - Identifikasi dampak *Flight Information Display System* (FIDS)

Kategori	Dampak
Confidentiality/ Kerahasiaan	Apabila aplikasi *Flight Information Display System* (FIDS) tidak memiliki hak akses bagi orang yang mempunyai hak akses saja dapat mengakibatkan pencurian data, perubahan data atau informasi/kerusakan data oleh pihak yang tidak bertanggung jawab karena aplikasi *Flight Information Display System* (FIDS) merupakan aplikasi yang memberikan informasi terkait jadwal penerbangan, data maskapai, data garbarata, dan pengendalian bagasi.
Integrity/ Keutuhan	Jika pihak yang tidak bertanggung jawab merubah informasi yang ada pada aplikasi *Flight Information Display System* (FIDS) dapat mengakibatkan informasi dan data yang dihasilkan menjadi tidak valid dan akurat yang menimbulkan kerugian bagi pihak operasional dan manajerial
Availability/ Ketersediaan	Apabila aplikasi *Flight Information Display System* (FIDS) tidak dapat diakses dimanapun dan kapanpun dapat mengakibatkan kerugian finansial bagi individu serta organisasi. Ketika aplikasi *Flight Information Display System* (FIDS) tidak dapat diakses maka proses informasi terkait penerbangan dapat berhenti dan menyebabkan gangguan bagi kelancaran proses bisnis pada instansi.

Tabel 4.4.3-4 - Identifikasi dampak Counter *check-in*

Kategori	Dampak
Confidentiality/ Kerahasiaan	Apabila aplikasi Counter *check-in* tidak memiliki hak akses bagi orang yang mempunyai hak akses saja dapat mengakibatkan pencurian data, perubahan data atau informasi/kerusakan data oleh pihak yang tidak bertanggung jawab karena aplikasi Counter *check-in* merupakan aplikasi informasi tentang data calon penumpang.
Integrity/ Keutuhan	Jika pihak yang tidak bertanggung jawab merubah informasi yang ada pada aplikasi Counter *check-in* dapat mengakibatkan informasi dan data yang dihasilkan menjadi tidak valid dan akurat yang menimbulkan kerugian bagi pihak operasional dan Manajerial
Availability/ Ketersediaan	Apabila aplikasi Counter *check-in* tidak dapat diakses dimanapun dan kapanpun dapat mengakibatkan kerugian finansial bagi individu serta organisasi. Ketika aplikasi Counter *check-in* tidak dapat diakses maka informasi yang dibutuhkan oleh calon penumpang dan tidak tersedia pada waktu yang dibutuhkan oleh karena itu dapat merugikan instansi dan menyebabkan gangguan bagi kelancaran proses bisnis pada instansi.

c. Dampak keamanan informasi Wifi ditunjukkan pada Tabel 4.4.3-5

Tabel 4.4.3-5 - Identifikasi dampak Wifi

Kategori	Dampak
Confidentiality / Kerahasiaan	Apabila wifi/*network* diakses oleh pihak yang tidak berkompeten dapat mengakibatkan Kerusakan pada salah satu *hardware* seperti *Switch, router* atau *hardware* utama pada wifi/*Network* sehingga jaringan yang ada pada instansi menjadi terganggu.
Integrity/ Keutuhan	Apabila salah satu perangkat dari wifi/network mengalami gangguan mengakibatkan jaringan pada instansi tidak dapat berjalan dengan baik sehingga informasi yang dari dapat tidak utuh
Availability/ Ketersediaan	Apabila wifi/*network* tidak tersedia, maka koneksi jaringan yang ada pada instansi/organisasi tidak dapat berjalan dengan baik akibatnya dapat mengganggu aktivitas bisnis dan mengganggu koneksi antar divisi dalam instansi terganggu.

d. Dampak keamanan informasi Wifi ditunjukkan pada Tabel 4.4.3-6

Tabel 4.4.3-6 – Identifikasi dampak router

Kategori	Dampak
Confidentiality/ Kerahasiaan	Apabila *router* dan *switch* diakses oleh pihak yang tidak berkompeten dapat mengakibatkan kerusakan pada salah *hardware (router* dan *switch)* utama pada *router* dan *switch* sehingga jaringan yang ada pada instansi menjadi terganggu
Integrity/ Keutuhan	Apabila salah satu perangkat dari *router* dan *switch* mengalami gangguan mengakibatkan jaringan pada instansi tidak dapat berjalan dengan baik sehingga informasi yang di dapat tidak utuh
Availability/ Ketersediaan	Apabila *router* dan *switch* tidak tersedia, maka koneksi jaringan yang ada pada instansi/organisasi tidak dapat berjalan dengan baik akibatnya dapat mengganggu aktifitas bisnis dan mengganggu koneksi antar divisi dalam instansi terganggu.

e. Dampak keamanan informasi Kabel ditunjukkan pada Tabel 4.4.3-7

Tabel 4.4.3-7 - Identifikasi dampak kabel jaringan

Kategori	Dampak
Confidentiality/ Kerahasiaan	Apabila kabel ubah oleh pihak yang tidak berkompeten dapat mengakibatkan kerusakan pada salah kabel utama pada *router* dan *switch* sehingga jaringan yang ada pada instansi menjadi terganggu
Integrity/ Keutuhan	Apabila salah satu perangkat dari kebel mengalami gangguan mengakibatkan jaringan pada instansi tidak dapat berjalan dengan baik sehingga informasi yang dari dapat tidak utuh

Availability/ Ketersediaan	Apabila kabel tidak tersedia, maka koneksi jaringan yang ada pada instansi/organisasi tidak dapat berjalan dengan baik akibatnya dapat mengganggu aktifitas bisnis dan mengganggu koneksi antar divisi dalam instansi terganggu.

f. Dampak keamanan informasi Data *Center* ditunjukkan pada Tabel 4.4.3-8

Tabel 4.4.3-8 - Identifikasi dampak data center

Kategori	Dampak
Confidentiality/ Kerahasiaan	Data *center* yang tidak memiliki hak akses bagi pihak yang tidak memiliki akses dapat menimbulkan dampak besar bagi individu maupun organisasi seperti penyalahgunaan data dan akses yang tidak diperbolehkan sehingga nantinya informasi yang tersedia dapat diketahui oleh pihak-pihak lain.
Integrity/ Keutuhan	Jika Data *center* yang diakses ilegal oleh pihak yang tidak bertanggung jawab dapat mengakibatkan perubahan informasi yang di sengaja sehingga informasi yang dihasilkan tidak valid dan tidak akurat.
Availability/ Ketersediaan	Data *center* tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak lain tidak memiliki akses pribadi bagi data pribadinya, data instansi dan pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggung jawab yang dapat Menyalah gunakan informasi yang tersedia.

g. Dampak keamanan informasi Data Jadwal Penerbangan ditunjukkan pada Tabel 4.4.3-9

Tabel 4.4.3-9 - Identifikasi dampak Data Jadwal Penerbangan

Kategori	Dampak
Confidentiality/ Kerahasiaan	Data Jadwal Penerbangan yang tidak memiliki hak akses bagi pihak yang tidak memiliki akses dapat menimbulkan dampak besar bagi individu maupun organisasi seperti penyalahgunaan data dan akses yang tidak diperbolehkan sehingga nantinya informasi yang tersedia dapat diketahui oleh pihak-pihak lain.
Integrity/ Keutuhan	Jika Data Jadwal Penerbangan yang diakses illegal oleh pihak yang tidak bertanggung jawab dapat mengakibatkan perubahan informasi yang disengaja sehingga informasi yang dihasilkan tidak valid dan tidak akurat.
Availability/ Ketersediaan	Jika Data Jadwal Penerbangan tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak lain tidak memiliki akses pribadi bagi data Jadwal dan pihak luar dapat mengetahui data-data penting terkait jadwal penerbangan yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggung jawab yang dapat menyalah gunakan informasi yang tersedia.

h. Dampak keamanan informasi Data Jadwal shift kerja pegawai ditunjukkan pada Tabel 4.4.3-10

Tabel 4.4.3-10 - Identifikasi dampak data Jadwal shift kerja pegawai

Kategori	Dampak
Confidentiality/ Kerahasiaan	Data Jadwal shift kerja pegawai yang tidak memiliki hak akses bagi pihak yang tidak memiliki akses dapat menimbulkan dampak besar bagi individu maupun organisasi seperti penyalahgunaan data dan akses yang tidak diperbolehkan sehingga nantinya informasi yang tersedia dapat diketahui oleh pihak-pihak lain.
Integrity/ Keutuhan	Jika Data Jadwal shift kerja pegawai yang diakses ilegal oleh pihak yang tidak bertanggung jawab dapat mengakibatkan perubahan informasi yang disengaja sehingga informasi yang dihasilkan tidak valid dan tidak akurat.
Availability/ Ketersediaan	seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggung jawab yang dapat menyalahgunakan informasi yang tersedia.

i. Dampak keamanan informasi Data Keuangan ditunjukkan pada Tabel 4.4.3-11 Tabel 4.4.3-11 - Identifikasi dampak data keuangan

Kategori	Dampak
Confidentiality/ Kerahasiaan	Data keuangan yang tidak memiliki hak akses bagi pihak yang tidak memiliki akses dapat menimbulkan dampak besar bagi individu maupun organisasi seperti penyalahgunaan data dan akses yang tidak diperbolehkan sehingga nantinya informasi yang tersedia dapat diketahui oleh pihak-pihak lain.
Integrity/ Keutuhan	Jika Data keuangan yang diakses ilegal oleh pihak yang tidak bertanggung jawab dapat mengakibatkan perubahan informasi yang disengaja sehingga informasi yang dihasilkan tidak valid dan tidak akurat.
Availability/ Ketersediaan	Jika Data keuangan tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak lain tidak memiliki akses pribadi bagi data pribadinya, data keuangan yang lain dan pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggung jawab yang dapat menyalahgunakan informasi yang tersedia.

j. Dampak keamanan informasi Data Perencanaan Pengadaan fasilitas bandara ditunjukkan pada Tabel 4.4.3-12

Tabel 4.4.3-12 - Identifikasi dampak Data Perencanaan Pengadaan fasilitas

bandara

Kategori	Dampak
Confidentiality/ Kerahasiaan	Data Perencanaan Pengadaan fasilitas bandara yang tidak memiliki hak akses bagi pihak yang tidak memiliki akses dapat menimbulkan dampak besar bagi individu maupun organisasi seperti penyalahgunaan data dan akses yang tidak diperbolehkan sehingga nantinya informasi yang tersedia dapat diketahui oleh pihak-pihak lain.
Integrity/ Keutuhan	Jika Data Perencanaan Pengadaan fasilitas bandara yang diakses ilegal oleh pihak yang tidak bertanggung jawab dapat mengakibatkan perubahan informasi yang disengaja sehingga informasi yang dihasilkan tidak valid dan tidak akurat.
Availability/ Ketersediaan	Jika Data Perencanaan Pengadaan fasilitas bandara tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggung jawab yang dapat menyalah gunakan informasi yang tersedia.

k. Dampak keamanan informasi Data Aset ditunjukkan pada Tabel. 4.4.3-13

Tabel 4.4.3-13 - Identifikasi dampak data aset

Kategori	Dampak
Confidentiality/ Kerahasiaan	Data Aset yang tidak memiliki hak akses bagi pihak yang tidak memiliki akses dapat menimbulkan dampak besar bagi individu maupun organisasi seperti penyalahgunaan data dan akses yang tidak diperbolehkan sehingga nantinya informasi yang tersedia dapat diketahui oleh pihak-pihak lain.
Integrity/ Keutuhan	Jika Data Aset yang diakses ilegal oleh pihak yang tidak bertanggung jawab dapat mengakibatkan perubahan informasi yang disengaja sehingga informasi yang dihasilkan tidak valid dan tidak akurat.
Availability/ Ketersediaan	Jika Data Aset tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak lain tidak memiliki akses pribadi bagi data pribadinya, data aset instansi dan pihak luar dapat mengetahui data- data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggung jawab yang dapat Menyalahgunakan informasi yang tersedia.

l. Dampak keamanan informasi Data Maskapai ditunjukkan pada Tabel 4.4.3-14

Tabel 4.4.3-14 - Identifikasi dampak Data Maskapai

Kategori	Dampak
Confidentiality/ Kerahasiaan	Data maskapai yang tidak memiliki hak akses bagi pihak yang tidak memiliki akses dapat menimbulkan dampak besar bagi individu maupun organisasi seperti penyalahgunaan data dan akses yang tidak diperbolehkan sehingga nantinya informasi yang tersedia dapat diketahui oleh pihak-pihak lain.
Integrity/ Keutuhan	Jika Data Maskapai yang diakses ilegal oleh pihak yang tidak bertanggungjawab dapat mengakibatkan perubahan informasi yang disengaja sehingga informasi yang dihasilkan tidak valid dan tidak akurat.
Availability/ Ketersediaan	Jika Data Maskapai tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggung jawab yang dapat menyalahgunakan informasi yang tersedia.

m. Dampak keamanan informasi Pengendalian Bagasi ditunjukkan pada Tabel 4.4.3-15

Tabel 4.4.3-15 - Identifikasi dampak Data Pengendalian Bagasi

Kategori	Dampak
Confidentiality/ Kerahasiaan	Data Pengendalian Bagasi yang tidak memiliki hak akses bagi pihak yang tidak memiliki akses dapat menimbulkan dampak besar bagi individu maupun organisasi seperti penyalahgunaan data dan akses yang tidak diperbolehkan sehingga nantinya informasi yang tersedia dapat diketahui oleh pihak-pihak lain.
Integrity/ Keutuhan	Jika Data Pengendalian Bagasi yang diakses ilegal oleh pihak yang tidak bertanggung jawab dapat mengakibatkan perubahan informasi yang disengaja sehingga informasi yang dihasilkan tidak valid dan tidak akurat.
Availability/ Ketersediaan	Jika Data Pengendalian Bagasi tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggung jawab yang dapat menyalahgunakan informasi yang tersedia.

n. Dampak keamanan informasi Operator Garbarata ditunjukkan pada Tabel 4.4.3-16

Tabel 4.4.3-16 - Identifikasi dampak Data Operator Garbarata

Kategori	Dampak
Confidentiality/ Kerahasiaan	Data Operator Garbarata yang tidak memiliki hak akses bagi pihak yang tidak memiliki akses dapat menimbulkan dampak besar bagi individu maupun organisasi seperti penyalahgunaan data dan akses yang tidak diperbolehkan sehingga nantinya informasi yang tersedia dapat diketahui oleh pihak-pihak lain.
Integrity/ Keutuhan	Jika Data Operator Garbarata yang diakses ilegal oleh pihak yang tidak bertanggung jawab dapat mengakibatkan perubahan informasi yang disengaja sehingga informasi yang dihasilkan tidak valid dan tidak akurat.
Availability/ Ketersediaan	Jika Data Operator Garbarata tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggung jawab yang dapat menyalahgunakan informasi yang tersedia.

o. Dampak keamanan informasi Hasil Evaluasi Layanan Bisnis Utama ditunjukkan pada Tabel 4.4.3-17

Tabel 4.4.3-17 - Identifikasi dampak Data Evaluasi Layanan Bisnis Utama

Kategori	Dampak
Confidentiality/ Kerahasiaan	Data Evaluasi Layanan Bisnis Utama yang tidak memiliki hak akses bagi pihak yang tidak memiliki akses dapat menimbulkan dampak besar bagi individu maupun organisasi seperti penyalahgunaan data dan akses yang tidak diperbolehkan sehingga nantinya informasi yang tersedia dapat diketahui oleh pihak-pihak lain.
Integrity/ Keutuhan	Jika Data Evaluasi layanan Bisnis Utama yang diakses ilegal oleh pihak yang tidak bertanggungjawab dapat mengakibatkan perubahan informasi yang disengaja sehingga informasi yang dihasilkan tidak valid dan tidak akurat.
Availability/ Ketersediaan	Jika Data Evaluasi Layanan Bisnis Utama tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggung jawab yang dapat menyalahgunakan informasi yang tersedia.

p. Dampak keamanan informasi Data Calon Penumpang ditunjukkan pada Tabel 4.4.3-18

Tabel 4.4.3-18 - Identifikasi dampak Data Calon Penumpang

Kategori	Dampak
Confidentiality/ Kerahasiaan	Data Calon Penumpang yang tidak memiliki hak akses bagi pihak yang tidak memiliki akses dapat menimbulkan dampak besar bagi individu maupun organisasi seperti penyalahgunaan data dan akses yang tidak diperbolehkan sehingga nantinya informasi yang tersedia dapat diketahui oleh pihak-pihak lain.
Integrity/ Keutuhan	Jika Data Calon Penumpang yang diakses ilegal oleh pihak yang tidak bertanggung jawab dapat mengakibatkan perubahan informasi yang disengaja sehingga informasi yang dihasilkan tidak valid dan tidak akurat.
Availability/ Ketersediaan	Jika Data Calon Penumpang tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggung jawab yang dapat menyalahgunakan informasi yang tersedia.

q. Dampak keamanan informasi SDM (Pegawai) ditunjukkan pada Tabel 4.4.3-19

Tabel 4.4.3-19 - Identifikasi dampak data pegawai (SDM)

Kategori	Dampak
Confidentiality/ Kerahasiaan	Pegawai yang tidak memiliki hak akses bagi pihak yang tidak memiliki akses dapat menimbulkan dampak besar bagi individu maupun organisasi seperti penyalahgunaan data dan akses yang tidak diperbolehkan sehingga nantinya informasi yang tersedia dapat diketahui oleh pihak-pihak lain.
Integrity/ Keutuhan	Jika Pegawai yang yang tidak bertanggung jawab mendapatkan akses ilegal oleh pihak yang tidak bertanggungjawab dapat mengakibatkan perubahan informasi yang disengaja sehingga informasi yang dihasilkan tidak valid dan tidak akurat.
Availability/ Ketersediaan	Jika akses Pegawai tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak lain tidak memiliki akses pribadi bagi data pribadinya, data aset instansi dan pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggung jawab yang dapat menyalahgunakan informasi yang tersedia.

r. Dampak keamanan informasi SDM (Satuan Pengamanan) ditunjukkan pada Tabel 4.4.3-20

Tabel 4.4.3-20 - Identifikasi dampak satuan pengamanan

Kategori	Dampak
Confidentiality/ Kerahasiaan	Satuan pengamanan yang tidak memiliki hak akses bagi pihak yang tidak memiliki akses dapat menimbulkan dampak besar bagi individu maupun organisasi seperti penyalahgunaan data dan akses yang tidak diperbolehkan sehingga nantinya informasi yang tersedia dapat diketahui oleh pihak-pihak lain.
Integrity/ Keutuhan	Jika Satuan pengamanan yang memiliki akses ilegal oleh pihak yang tidak bertanggungjawab dapat mengakibatkan perubahan informasi yang disengaja sehingga informasi yang dihasilkan tidak valid dan tidak akurat.
Availability/ Ketersediaan	Jika Satuan pengamanan tidak tersedia maka pihak lain dapat mengakses keamanan bagi data pribadinya atau data instansi dan pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggung jawab yang dapat menyalahgunakan informasi yang tersedia.

4.5.1 Lanjutan tabel analisa dampak bisnis

Tabel 4.5.1 – Analisa Dampak Bisnis

No.	Kategori Aset	Daftar Aset	Dampak	Nilai BIA	Skala BIA
1.	*Hardware*	*Server*	Operasi layanan aplikasi pusat dan unit terhenti	4	*Very high critical*
		PC	Pelaporan data pada aplikasi individu tertunda karena gangguan PC	3	*High critical*
2.	Software	*Flight Information Display system*	Proses bisnis bandara terganggu seperti jadwal penerbangan, jadwal operator garbarata, layanan bagasi *handling*.	4	*Very high critical*
		Counter check-in	Proses *check-in* calon penumpang terganggu	4	*Very high critical*

3.	Jaringan	Wifi	Apabila *network* tidak tersedia, maka koneksi jaringan yang ada pada instansi tidak dapat berjalan dengan baik, akibatnya dapat mengganggu aktifitas bisnis perusahaan dan koneksi antar divisi dalam instansi terganggu	3	*High critical*
		Router dan Switch	Apabila *router/switch* tidak tersedia, maka koneksi jaringan yang ada pada instansi tidak dapat berjalan dengan baik, akibatnya dapat mengganggu aktifitas bisnis perusahaan dan koneksi antar divisi dalam instansi terganggu	3	*High critical*
		Kabel	Apabila kabel tidak tersedia, maka koneksi jaringan yang ada pada instansi tidak dapat berjalan dengan baik, akibatnya dapat mengganggu aktifitas bisnis perusahaan dan koneksi antar divisi dalam instansi terganggu	3	*High critical*
4.	Data	Data *center*	Data *center* tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak lain tidak memiliki akses pribadi bagi data pribadinya, data instansi dan pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggung jawab yang dapat Menyalahgunakan informasi yang tersedia.	4	*Very high critical*
		Data Jadwal Penerbangan	Jika Data Jadwal Penerbangan yang diakses illegal oleh pihak yang tidak bertanggung jawab dapat mengakibatkan perubahan informasi yang disengaja sehingga informasi yang dihasilkan tidak valid dan tidak akurat.	4	*Very high critical*
		Data Jadwal Shift Kerja Pegawai	Jika Data Jadwal shift kerja pegawai tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak lain tidak memiliki akses pribadi bagi data pribadinya, data pegawai yang lain dan pihak luar	3	*High critical*

		Data Perencanaan Pengadaan Fasilitas Bandara	Jika Data Perencanaan Pengadaan fasilitas bandara tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggung jawab yang dapat menyalahgunakan informasi yang tersedia.	3	*High critical*
		Data Maskapai	Jika Data Maskapai tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggung jawab yang dapat menyalahgunakan informasi yang tersedia.	3	*High critical*
		Data Keuangan	Jika Data keuangan tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak lain tidak memiliki akses pribadi bagi data pribadinya, data keuangan yang lain dan pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggung jawab yang dapat menyalahgunakan informasi yang tersedia.	3	*High critical*
		Data PengendalianBagasi	Jika Data Pengendalian Bagasi tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggung jawab yang dapat menyalahgunakan informasi yang tersedia.	4	*Very high critical*

		Data Operator Garbarata	Jika Data Operator Garbarata tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggung jawab yang dapat menyalahgunakan informasi yang tersedia.	4	*Very high critical*
		Data Hasil Evaluasi Tiap Layanan Bisnis Utama	Jika Data Evaluasi Layanan Bisnis Utama tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggung jawab yang dapat menyalahgunakan informasi yang tersedia.	3	*High critical*
		Data Calon Penumpang	Jika Data Calon Penumpang tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggung jawab yang dapat menyalahgunakan informasi yang tersedia.	4	*Very high critical*
		Data Asset	Pelaporan monitoring aset instansi tertunda	2	*Mayor critical*
5.	SDM	Pegawai	Pengguna tidak mempunyai kontrol akses sehingga dapat menimbulkan akses ilegal oleh pihak lain	3	*High critical*
		Satuan Pengamanan	Kelalaian petugas dapat menimbulkan dampak negatif bagi instansi	2	*Mayor critical*

4.5.2 Lanjutan Tabel Identifikasi Level Risiko

Tabel 4.5.2 – Identifikasi level risiko

No.	Kategori Aset	Daftar Aset	Nilai Ancaman	Skala BIA	Level Risiko
1.	*Hardware*	*Server*	0,4 *(high)*	*Very high critical*	*High* 100
		PC	0,48 *(high)*	*High critical*	*High* 80
2.	*Software*	*Flight Information Display System* (FIDS)	0,5 (*high*)	*Very high critical*	*High* 100
		Counter check-in	0,43 (*high)*	*Very high critical*	*High* 100
3.	Jaringan	Wifi	0,57 (*high)*	*High critical*	*High* 80
		Router dan switch	0,51 (*high)*	*High critical*	*High* 80
		Kabel	0,57 (*high)*	*High critical*	*High* 80
4.	Data	Data *center*	0,48 (*high)*	*Very High critical*	*High* 100
		Data Jadwal Penerbangan	0,43 *(high)*	*Very High critical*	*High* 100
		Data jadwal shift kerja pegawai	0,4 *(high)*	*High critical*	*High* 80
		Data maskapai	0,45 *(high)*	*High critical*	*High* 80
		Data perencanaan pengadaan fasilitas bandara	0,35 *(medium)*	*High critical*	*High* 80
		Data keuangan	0,4 *(high)*	*High critical*	*High* 80
		Data pengendalian bagasi	0,53 *(high)*	*Very High critical*	*High* 100
		Data operator garbarata	0,38 *(medium)*	*Very High critical*	*High* 100

		Data hasil evaluasi tiap layanan bisnis utama	0,37 *(medium)*	*High critical*	*High* 80
		Data aset	0,45 *(high)*	*Mayor critical*	*Medium* 30
		Data calon penumpang	0,4 *(high)*	*Very High critical*	*High* 100
		Data pegawai	0,35 *(medium*)	*High critical*	*High* 80
5.	SDM	Data satuan pengamanan	0,2 *(medium)*	*Mayor critical*	*Medium* 30

4.5.3 Lanjutan Tabel Menentukan Level Risiko diterima atau perlu penanganan risiko

Tabel 4.5.3 penentuan risiko

No.	Kategori Aset	Daftar Aset	Nilai Aset (NA)	Nilai BIA (BIA)	Nilai Ancaman (NT)	Nilai Risiko (NA x BIA x NT)
1.	*Hardware*	*Server*	11	4	0,4	17,6
		PC	9	3	0,48	12,96
2.	*Software*	*Flight Information Display System* (FIDS)	12	4	0,5	24
		Counter check-in	12	4	0,43	20,64
3.	Jaringan	Wifi	7	3	0,57	11,97
		Router dan Switch	9	3	0,51	13,77
		Kabel	8	3	0,57	13,68
4	Data	Data *center*	12	4	0,48	23,04
		Data Jadwal penerbangan	12	4	0,43	20,04
		Data jadwal shift kerja pegawai	9	3	0,4	10,8
		Data Maskapai	12	4	0,45	21,6
		Data Perencanaan pengadaan fasilitas bandara	12	3	0,35	12,6
		Data Keuangan	12	4	0,4	19,2

		Data pengendalian bagasi	12	4	0,53	25,44
		Data operator garbarata	11	4	0,38	16,72
		Data hasil evaluasi tiap layanan bisnis utama	12	3	0,37	13,32
		Data Aset	12	2	0,45	10,8
		Data calon penumpang	12	4	0,4	19,2
5.	SDM	Pegawai	10	3	0,35	10,5
		Satuan Pengamanan	9	2	0,2	3,6

Setelah dapat diketahui nilai risiko pada masing-masing aset, langkah selanjutnya yaitu menentukan level risiko pada masing-masing aset. Penentuan level risiko dilakukan dengan menyesuaikan hasil dari nilai risiko pada matriks level risiko pada Tabel 4.5.2 yang telah dibuat sebelumnya. Hasil dari level risiko dari masing-masing aset ditunjukkan pada Tabel 4.5.3-1

Tabel 4.5.3-1 – level risiko

No.	Kategori Aset	Daftar Aset	Nilai Risiko (NA x BIA x NT)	Level Risiko
1.	*Hardware*	*Server*	17,6	*High*
		PC	12,96	*Medium*
2.	*Software*	*Flight Information Display System* (FIDS)	24	*High*
		Counter check-in	20,64	*High*
3.	Jaringan	Wifi	11,97	*Medium*
		Router dan Switch	13,77	*Medium*
		Kabel	13,68	*Medium*
4.	Data	Data *center*	23,04	*High*
		Data Jadwal penerbangan	20,04	*High*
		Data jadwal shift kerja pegawai	10,8	*Medium*
		Data Maskapai	21,6	*High*

		Data Perencanaan pengadaan fasilitas bandara	12,6	*Medium*
		Data keuangan	19,2	*Medium*
		Data pengendalian bagasi	25,44	*High*
		Data operator garbarata	16,72	*Medium*
		Data hasil evaluasi tiap layanan bisnis utama	13,32	*Medium*
		Data Aset	10,8	*low*
		Data calon penumpang	19,2	*Medium*
5.	SDM	Pegawai	10,5	*Low*
		Satuan Pengamanan	3,6	*Low*

Dari hasil level risiko diatas, maka dapat ditentukan ada beberapa aset yang bernilai High yaitu Server, *Flight Information Display System* (FIDS), counter *check-in*, data center, data jadwal penerbangan, data maskapai, dan data pengendalian bagasi. Adapun beberapa aset yang bernilai Medium yaitu PC, Wifi, Router, kabel, data shift kerja pegawai, pegawai (SDM), data pengadaan fasilitas, data keuangan, data operator garbarata, data evaluasi tiap layanan bisnis utama, dan data calon penumpang. Adapun beberapa aset yang bernilai Low yaitu data aset, satuan pengamanan dan pegawai. risiko dilakukan dengan asset yang bernilai high, medium dan low sesuai dengan kriteria penerimaan risiko yang telah dibuat pada sub tahapan sebelumnya.

4.6.1 lanjutan Tabel Memilih Kontrol Objektif dan Kontrol Keamanan

Tabel 4.6.1 - Pemetaan Kontrol objektif dan Kontrol keamanan

No.	Klausul	Kontrol Objektif	Kontrol Keamanan
1.	A.5 – Kebijakan Keamanan	A.5.1 – Arahan manajemen untuk	A.5.1.1 Kebijakan untuk keamanan informasi

	Informasi	keamanan informasi	5.1.2 Tinjauan kebijakan untuk keamanan informasi
2.	A.6 – Organisasi Keamanan Informasi	A.6.1 Organisasi internal	A.6.1.1 Peran dan tanggung jawab keamanan informasi
3.	A.7 - Keamanan SDM	A.7.1 – sebelum bekerja	A.7.1.2. Syarat dan ketentuan kerja
		A.7.2 – selama bekerja	A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi
4.	A.8 – Manajemen Aset	A.8.1 –Tanggung Jawab Asset	A.8.1.1 Inventarisasi Terhadap Asset
5.	A.9 - Kontrol Akses	A.9.1 – persyaratan bisnis untuk kontrol akses	A.9.1.1 Kebijakan pengendalian kontrol akses
		A.9.2 – Manajemen Hak pengguna	A.9.2.3 Manajemen hak akses khusus
		A.9.3 – Tanggung jawab pengguna	A.9.3.1 Penggunaan informasi autentikasi rahasia
		A.9.4 – Sistem dan kontrol akses aplikasi	A.9.4.1 Pembatasan akses Informasi
			A.9.4.2 Prosedur *log-on* yang Aman
			A.9.4.3 Sistem manajemen *Password*
6.	A.10 – Kriptografi	A.10.1 – Kontrol Kriptografi	A.10.1.1 Kebijakan dalam penggunaan control kriptografi
7.	A.11 - Fisik dan Keamanan Lingkungan	A.11.2 – Peralatan	A.11.2.3 Pengendalian keamanan kabel
			A.11.2.4 Kontrol pemeliharaan Peralatan
		A.12.3 – *Backup*	A.12.3.1 *Backup* informasi
			A.12.4.1 Pencatatan kejadian

8.	A.12 – Keamanan Operasional	A.12.4 – *Logging* dan pemantauan	A.12.4.2 Perlindungan informasi *Log*
			A.12.4.3 *Log* administrasi dan Operator
9.	A.17–Manajemen Kelangsungan bisnis	A.17.1 Aspek keamanan Dalam manajemen Kelangsungan bisnis	A.17.1.1 memasukkan keamanan informasi dalam proses manajemen kelangsungan bisnis

Pada tabel 4.6.1-1 berikut adalah pemetaan risiko dan kontrol objektif dan kontrol keamanan ISO 27001:2013, untuk lebih lengkapnya kebutuhan kontrol objektif dan kontrol keamanan dapat dilihat pada lampiran 6 Pemetaan hasil rekomendasi pengendalian Risiko dengan kebutuhan pada ISO 27001:2013.

Tabel 4.6.1.-1 – pemetaan risiko dengan kebutuhan keamanan

Kategori Aset	Aset Potensi kegagalan	Potensi penyebab kegagalan	Kontrol Keamanan
Hardware	Kerusakan *Server*	Kesalahan konfigurasi *server*	A.11.2.4 Kontrol pemeliharaan peralatan
	Kerusakan PC	Kesalahan konfigurasi PC	
Data	Data Hilang	Kelalaian Teknisi	A.9.1.1 Kebijakan pengendalian kontrol akses
			A.9.3.1 Penggunaan informasi autentikasi rahasia
			A.12.4.3 *Log* administrasi dan operator
		Aset tidak di pelihara	A.8.1.1 Inventarisasi Terhadap aset
		Kebocoran Informasi	A.10.1.1kebijakan dalam Penggunaan kontrol Kriptografi
	Manipulasi Data	Rusaknya media penyimpanan	A.12.3.1 *Backup* informasi
			A.11.2.4 Kontrol pemeliharaan peralatan
		Username password diketahui orang lain	A.9.1.1 Kebijakan pengendalian kontrol akses
			A.9.2.3 Manajemen hak akses khusus

			A.9.4.2 Prosedur *log-on* yang aman
			A.9.4.3 Sistem manajemen *Password*
Informasi	Kesalahan penyampaian informasi	Adanya kesalahan dalam penyampaian informasi akibat Kelalaian pegawai	A.5.1.1 Kebijakan untuk keamanan informasi
			5.1.2 Tinjauan kebijakan untuk keamanan informasi
		Manajemen Kelangsungan bisnis	A.17.1 Aspek Keamanan Informasi dalam manajemen kelangsungan bisnis
		Adanya kesalahan tanggung jawab peran dalam penyampaian Informasi	A.6.1.1 Peran dan tanggung jawab keamanan informasi
Software	Aplikasi diakses oleh pihak yang tidak berwewenang	User dan *password* diketahui oleh pengguna lain	A.9.1.1 Kebijakan pengendalian kontrol akses
			A.9.4.1 Pembatasan akses Informasi
			A.9.4.2 Prosedur *log-on* yang aman
			A.9.4.3 Sistem manajemen *Password*
Jaringan	Kerusakan kabel LAN	Kurangnya kontrol pengamanan kabel	A.11.2.3 Pengendalian keamanan kabel
SDM	Sharing *password*	Kelalaian pegawai yang memiliki hak akses	A.7.1.2. Syarat dan ketentuan kerja
			A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi
			A.9.1.1 Kebijakan pengendalian kontrol akses
	Data tidak sesuai (tidak valid)	Kesalahan input data	A.12.4.1Pencatatan Kejadian
			A.12.4.2 Perlindungan informasi *log*

Berdasarkan hasil Pemetaan rekomendasi penyesuaian pengendalian risiko, didefinisikan beberapa prosedur yang dapat diusulkan dalam penelitian dengan hasil penilaian yang telah dilakukan maka penulis melakukan pembuatan dokumen kebijakan yang telah dilakukan oleh instansi terlebih dahulu. Dengan begitu,

diharapkan dokumen prosedur, kebijakan, dan instruksi kerja yang telah dibuat dapat dijalankan dengan baik dalam manajemen keamanan informasi. Berikut ini adalah hasil pemetaan risiko dengan klausul dan kategori kebutuhan keamanan informasi dapat dilihat pada tabel Tabel 4.6.1.-2.

Tabel Tabel 4.6.1.-2 - Pemetaan Risiko dengan klausul dan kategori kebutuhan

No.	Kategori Aset	Risiko yang terjadi	Klausul	Kontrol Objektif	Kontrol Keamanan	Kategori Kebutuhan
1.	Data	Adanya data yang hilang disebabkan oleh kelalaian pegawai yang memiliki hak akses	A.9 - Kontrol Akses	A.9.1 – persyaratan bisnis untuk kontrol Akses	A.9.1.1 Kebijakan pengendalian kontrol akses	Teknikal
				A.9.3 – Tanggung jawab pengguna	A.9.3.1 Penggunaan informasi autentikasi rahasia	
			A.12 - Keamanan Operasional	A.12.4 – *Logging* dan pemantauan	A.12.4.3 *Log* administrasi dan operator	Operasional
		Adanya data yang hilang disebabkan kurangnya manajemen aset	A.8 – Manajemen Aset	A.8.1 – Tanggung jawab aset	A.8.1.1 – Inventarisasiterhadap aset	Manajemen
		Adanya manipulasi data akibat Username dan password diketahui pengguna lain	A.9 - Kontrol Akses	A.9.1 – persyaratan bisnis untuk kontrol akses	A.9.1.1 Kebijakan pengendalian kontrol akses	Teknikal
		Adanya manipulasi data	A.9 - Kontrol Akses	A.9.4 – Sistem dan kontrol akses aplikasi	A.9.4.1 Pembatasan akses informasi	

		disebabkan oleh Username dan password diketahui pengguna lain			A.9.4.2 Prosedur *log- on* yang aman	
			A.9 - Kontrol Akses	A.9.4 – Sistem dan kontrol akses aplikasi	A.9.4.3 Sistem manajemen *password*	
		Rusaknya media penyimpanan (file data)	A.11 - Fisik dan keamanan Lingkungan	A.11.2 – Peralatan	A.11.2.4 Kontrol pemeliharaan peralatan	Teknikal
		Kesalahan input data	A.12 - Keamanan Operasional	A.12.3 – *Backup*	A.12.3.1 *Backup* informasi	Operasional
			A.12 - Keamanan Operasional	A.12.4 – *Logging* dan pemantauan	A.12.4.1 Pencatatan kejadian	
					A.12.4.2 Perlindungan informasi *log*	
2.	Informasi	Adanya kesalahan dalam penyampaian informasi disebabkan oleh kelalaian pegawai	A.5 – Kebijakan Keamanan Informasi	A.5.1 – Arahan manajemen untuk keamanan informasi	A.5.1.1 Kebijakan untuk keamanan informasi	Manajemen
		Adanya kesalahan tanggung jawab peran dalam penyampaian informasi	A.6 – Organisasi Keamanan Informasi	A.6.1 Organisasi internal	A.6.1.1 Peran dan tanggung jawab	
3.	*Hardware*	Kesalahan konfigurasi *server*	A.11 - Fisik dan Keamanan Lingkungan	A.11.2 – Peralatan	A.11.2.4 Kontrol pemeliharaan peralatan	Teknikal

		Kesalahan konfigurasi PC				
4.	Jaringan	Kurangnya kontrol pengamanan kabel	A.11 - Fisik dan Keamanan Lingkungan	A.11.2 – Peralatan	A.11.2.3 Pengendalian keamanan kabel	Teknikal
5.	*Software*	Aplikasi diakses oleh pihak yang tidak berwewenang	A.9 - Kontrol Akses	A.9.1 – persyaratan bisnis untuk kontrol akses	A.9.1.1 Kebijakan pengendalian kontrol akses	Teknikal
		Username dan password diketahui oleh pengguna lain		A.9.4 – Sistem dan kontrol akses aplikasi	A.9.4.2 Prosedur *log-on* yang aman	
				A.9.4 – Sistem dan kontrol akses Aplikasi	A.9.4.3 Sistem manajemen *password*	
6.	SDM	Kelalaian pegawai yang memiliki hak akses	A.9 - Kontrol Akses	A.9.1 – persyaratan bisnis untuk kontrol Akses	A.9.1.1 Kebijakan pengendalian kontrol akses	Teknikal
				A.9.3 – Tanggung jawab pengguna	A.9.3.1 Penggunaan informasi autentikasi rahasia	
			A.12 - Keamanan Operasional	A.12.4 – *Logging* dan pemantauan	A.12.4.3 *Log* administrasi dan operator	Operasional
			A.7 - Keamanan SDM	A.7.1 – sebelum bekerja	A.7.1.2. Syarat dan ketentuan kerja	Teknikal

				A.7.2 – selama bekerja	A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi	Teknikal

Pada tabel Tabel 4.6.1.-3 berikut adalah pemetaan risiko dengan dokumen kebijakan yang dihasilkan dengan pemilihan kontrol keamanan yang sesuai.

Tabel Tabel 4.6.1.-3 – Pemetaan Risiko dengan Dokumen Kebijakan

No	Kategori Aset	Risiko yang terjadi	Kategori Kebutuhan	Kontrol Keamanan	Dokumen Kebijakan
1.	Data	Adanya data yang hilang akibat Kelalaian pegawai yang memiliki hak akses	Teknikal	A.9.1.1 Kebijakan pengendalian kontrol akses	KB 01 Pengendalian Hak Akses
				A.9.3.1 Penggunaan informasi autentikasi rahasia	KB 04 *Human resources Security*
			Operasional	A.12.4.3 *Log* administrasi dan operator	KB 02 Keamanan informasi (point4.1 dan 4.2)
		Adanya manipulasi data akibat *Username* dan *password* diketahui pengguna lain	Teknikal	A.9.1.1 Kebijakan pengendalian kontrol akses	KB 01 Pengendalian Hak Akses
		Adanya manipulasi data akibat Username dan password diketahui pengguna lain		A.9.4.1 Pembatasan akses informasi	KB 02 Keamanan informasi (point 4.2 dan 4.3)

				A.9.4.2 Prosedur *log- on* yang aman	
				A.9.4.3 Sistem manajemen *password*	
		Rusaknya media penyimpanan (file data)	Teknikal	A.11.2.4 Kontrol pemeliharaan peralatan	KB 03 Pengelolaan hardware dan kabel jaringan telekomunikasi
			Manajemen	A.8.1.1 Inventarisasi terhadap aset	KB 02 Keamanan informasi (point 4.1)
		Kesalahan input data	Operasional	A.12.3.1 *Backup* informasi	KB 02 Keamanan informasi (point 4.1)
				A.12.4.1 Pencatatan kejadian	KB 02 Keamanan informasi (poin 4.1 dan 4.2)
				A.12.4.2 Perlindungan informasi *log*	
2.	Informasi	Adanya kesalahan Dalam penyampaian informasi akibat Kelalaian pegawai	Manajemen	A.5.1.1 Kebijakan untuk keamanan informasi	KB 02 Keamanan dan pengendalian informasi (point 4.5)
		Adanya kesalahan tanggung jawab peran dalam penyampaian informasi		A.6.1.1 Peran dan tanggung jawab	

3.	*Hardware*	Kesalahan konfigurasi *server* kesalahan konfigurasi *server*	Teknikal	A.11.2.4 Kontrol Pemeliharaan Peralatan	KB 03 Pengelolaan hardware dan kabel jaringan telekomunikasi
		Kesalahan konfigurasi PC			
4.	Jaringan	Kurangnya kontrol pengamanan kabel	Teknikal	A.11.2.3 Pengendalian keamanan kabel	KB 03 Pengelolaan hardware dan kabel jaringan telekomunikasi
5.	*Software*	Aplikasi diakses oleh pihak yang tidak berwewenang	Teknikal	A.9.1.1 Kebijakan pengendalian kontrol akses	KB 01 Pengendalian Hak akses
		Username dan password diketahui oleh pengguna lain		A.9.4.2 Prosedur *log- on* yang aman	KB 02 Keamanan informasi (poin 4.2 dan 4.3)
				A.9.4.3 Sistem manajemen *password*	
6.	SDM	Kelalaian pegawai yang memiliki hak akses	Teknikal	A.9.1.1 Kebijakan pengendalian kontrol akses	KB 01 Pengendalian Hak akses
				A.9.3.1 Penggunaan informasi autentikasi rahasia	KB 04 Human resources security
			Operasional	A.12.4.3 *Log* administrasi dan operator	KB 02 Keamanan informasi (poin 4.1 dan 4.2)
			Teknikal	A.7.1.2. Syarat dan ketentuan kerja	KB 04 Human resources security
				A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi	

Pada tabel Tabel 4.6.1.-4 berikut adalah pemetaan kebijakan dengan dokumen prosedur, Instruksi kerja dan formulir yang dihasilkan.

Keterangan:

KB : Kebijakan

PO : Prosedur

IK : Instruksi Kerja

FM : Formulir

pemetaan risiko dengan dokumen kebijakan yang dihasilkan dengan pemilihan kontrol keamanan dapat dilihat pada tabel Tabel 4.6.1.-4. Berdasarkan kategori aset data adanya risiko yaitu hilangnya data disebabkan oleh kelalaian pegawai yang memiliki hak akses dari risiko tersebut kebutuhan kategori yaitu teknikal dengan kontrol keamananA.9.1.1danA.9.3.1 dihasilkan 2 dokumen kebijakan yaitu KB-01 pengendalian hak akses dan KB-04 *Human resources security*.

Pada tabel Tabel 4.6.1.-4 berikut adalah pemetaan hasil kebijakan dengan prosedur, instruksi kerja dan formulir.

Tabel Tabel 4.6.1.-4 - Pemetaan kebijakan dengan prosedur, instruksi kerja dan formulir

Kebijakan	Prosedur	Instruksi Kerja	Formulir
KB 01 Pengendalian Hak akses	PO 01 Pengelolaan hak akses	IK 01 Perubahan Hak Akses - Pemberian hak akses - Penghapusan hak akses - Perubahan hak akses	FM 01: pengelolaan hak akses FM 02: kontrak perjanjian hak akses FM 03: *log – on* pengelolaan hak akses
KB 04 *Human resources security*	PO 06 Pelatihan dan pengembangan SDM	IK 08 Pelatihan dan pengembangan SDM - Proses pendaftaran pelatihan dan pengembangan - proses persiapan pelatihan dan pengembangan - proses pelatihan dan pengembangan - evaluasi pelatihan dan pengembangan	FM 12: Data pegawai FM 13: Evaluasi kegiatan pelatihan dan pengembangan

Tabel 4.6.1.-4 (Lanjutan)

Kebijakan	Prosedur	Instruksi Kerja	Formulir
KB 04 *Human resources security*	PO 09 Manajemen asset informasi	IK - 09 Klasifikasi Keamanan informasi	FM 14: Monitoring Keamanan informasi
KB 02 – point 4.1 dan 4.2 Keamanan informasi	PO 03 *Backup dan Restore*	IK - 04 Backup data dan file - *backup database* - *backup file*	FM 06 : Klasifikasi data FM 07: *log backup* data
		IK 05 *Restore* data	FM 08: *restore* data
	PO 07 Keamanan Informasi	IK 09 Klasifikasi Keamanan informasi	FM 14: Monitoring Keamanan informasi
KB 01 Pengendalian Hak akses	PO 01 Pengelolaan hak akses	IK 01 - Perubahan Hak Akses - Pemberian hak akses - Penghapusan hak akses - Perubahan hak akses	FM 01: pengelolaan hak akses FM 02: kontrak perjanjian hak akses FM 03: *log-on* pengelolaan hak akses
KB 02 – point 4.2 dan 4.3 Keamanan informasi	PO 02 Pengelolaan *password*	IK 02 Perubahan *password*	FM 04: perbaikan sistem informasi
		IK 03 *Reset password*	FM 05: *reset password*
	PO 04 Pengelolaan *hardware*	IK 06 Perawatan *Hardware*: - Pelaporan kerusakan *hardware* - Pemeliharaan *Hardware* - Perbaikan *hardware*	FM 04: Perbaikan Sistem
KB 03 Pengelolaan *hardware*			Informasi FM 09: Pemeliharaan perangkat

dan kabel jaringan telekomunikasi	PO 05 Pengelolaan kabel jaringan telekomunikasi	IK 07 Perawatan kabel jaringan telekomunikasi: - Pemeliharaan kabel Telekomunikasi - Pelaporan kerusakan kabel telekomunikasi	TI FM 10 : Berita acara kerusakan FM 11: Laporan Evaluasi penggunaan perangkat TI
KB 02 - Point 4.1 Keamanan informasi	PO 02 Pengelolaan *password*	IK 02 Perubahan password	FM 04 : perbaikan sistem informasi
		IK 03 *Reset password*	FM 05: *reset password*
KB 02 - point 4.1 dan 4.2 Keamanan informasi	PO 03 *Backup dan Restore*	IK 04 *Backup* data dan file - *backup database* - *backup file*	FM 06: Klasifikasi data FM 07: *log backup* Data
		IK 05 *Restore* data	FM 08: *restore* data
KB 02 - point 4.5 keamanan dan pengendalian informasi	PO 07 Keamanan informasi	IK 09 Klasifikasi Keamanan informasi	FM 14: Monitoring Keamanan informasi
		10 Peran dan tanggung jawab informasi	
KB 03 Pengelolaan *hardware* dan kabel jaringan telekomunikasi	PO 04 Pengelolaan *hardware*	IK 06 Perawatan *Hardware:* - Pelaporan kerusakan *hardware* - Pemeliharaan *hardware* - Perbaikan *hardware*	FM 04: Perbaikan Sistem informasi FM 09: Pemeliharaan perangkat TI FM 10 : Berita acara kerusakan FM 11: Laporan Evaluasi penggunaan perangkat TI

KB 03 Pengelolaan *hardware* dan kabel jaringan telekomunikasi	PO 05 Pengelolaan kabel jaringan telekomunikasi	IK 07 Perawatan kabel jaringan telekomunikasi: - Pemeliharaan kabel telekomunikasi - Pelaporan kerusakan kabel telekomunikasi - perbaikan kabel telekomunikasi	FM 04: Perbaikan Sistem informasi FM 09: Pemeliharaan perangkat TI FM 10: Berita acara kerusakan FM 11: Laporan Evaluasi penggunaan perangkat TI
KB 01 Pengendalian Hak akses	PO 01 Pengelolaan hak akses	IK 01 Perubahan Hak Akses - Pemberian hak akses - Penghapusan hak akses - Perubahan hak akses	FM 01: pengelolaan hak akses FM 02: kontrak perjanjian hak akses FM 03: *log-on* pengelolaan hak akses
KB 02 – point 4.2 dan 4.3 Keamanan Informasi	PO 02 Pengelolaan *password*	IK 02 Perubahan *password* IK 03 *Reset password*	FM 04: perbaikan sistem informasi FM 05: *reset password*
KB 01 Pengendalian Hak akses	PO 01 Pengelolaan hak akses	IK 01 Perubahan Hak Akses - Pemberian hak akses - Penghapusan hak akses - Perubahan hak akses	FM 01: pengelolaan hak akses FM 02: kontrak perjanjian hak akses FM 03: *log-on* pengelolaan hak akses
KB 04 *Human resources security*	PO 06 Pelatihan dan pengembangan SDM	IK 08 Pelatihan dan pengembangan SDM - Proses pendaftaran Pelatihan dan pengembangan - proses persiapan Pelatihan dan pengembangan - proses Pelatihan dan pengembangan - evaluasi Pelatihan dan pengembangan	FM 12: Data pegawai FM 13: Evaluasi kegiatan pelatihan dan pengembangan

KB 02 – point 4.1 dan 4.2 Keamanan informasi	PO 03 *Backup dan Restore*	IK 04 Backup data dan file - *backup database* - *backup file*	FM 06: Klasifikasi data FM 07: *log backup* Data
		IK 05 *Restore* data	FM 08: restore data
KB 04 *Human resources security*	PO 06 Pelatihan dan pengembangan SDM	IK 08 Pelatihan dan pengembangan SDM - Proses pendaftaran pelatihan dan pengembangan proses persiapan Pelatihan dan pengembangan proses Pelatihan dan pengembangan - evaluasi Pelatihandan pengembangan	FM 12: Data pegawai FM 13: Evaluasi kegiatan pelatihan dan pengembangan

Berdasarkan tabel 4.6.1.-4 berikut adalah salah satu contoh pembahasan dari pemetaan risiko dengan dokumen kebijakan yang dihasilkan dengan pemilihan kontrol keamanan dapat dilihat pada tabel 4.6.1-4. Berdasarkan kategori aset data adanya risiko yaitu hilangnya data disebabkan oleh kelalaian pegawai yang memiliki hak akses dari risiko tersebut kebutuhan kategori yaitu teknikal dengan control keamanan A.9.1.1dan A.9.3.1dihasilkan 2 dokumen kebijakan yaitu KB 01 pengendalian hak akses dan KB-04 *Human resources security* serta dokumen pendukung yaitu 2 prosedur PO 01 Pengelolaan hak akses dan PO 02 Pelatihan dan pengembangan SDM, 2 instruksi kerja yaitu IK-01 Perubahan hak akses dan IK 08 Pelatihan dan pengembangan SDM dan 5 formulir yang dihasilkan yaitu FM 01 pengelolaan hak akses, FM 02 kontrak perjanjian hak akses, FM 03 *log-on* pengelolaan hak akses, FM 12 Data pegawai, dan FM 13 Evaluasi kegiatan pelatihan dan pengembangan.

4.7.2 Lanjutan penjelasan pembentukan prosedur dan kebijakan

Kebijakan pengendalian hak akses Kebijakan ini dibuat berdasarkan risiko dan hasil rekomendasi pengendalian risiko yang sudah dilakukan dimana risiko yang teridentifikasi sebagai berikut:

a. Aplikasi diakses oleh pihak tidak berwenang
b. *Sharing password* karena kelalaian pegawai
c. Adanya manipulasi data karena *username password* diketahui orang lain

Berdasarkan risiko yang dijelaskan peneliti menentukan dengan membuat kebijakan pengendalian hak akses yang menggunakan acuan ISO27001:2013 pada klausul A.9.1.1 Kebijakan pengendalian kontrol akses yang berisikan mengenai pedoman peraturan hak akses yang diberikan, selain itu instansi juga belum memiliki dokumen kebijakan tertulis mengenai hak akses. Kebijakan ini terkait juga dengan prosedur pengelolaan hak akses.

A. **Prosedur pengelolaan hak akses**

Prosedur ini dibuat karena tidak adanya prosedur operasional secara tertulis pada instansi, prosedur ini menjelaskan langkah-langkah/aktivitas yang harus dilakukan dan dokumen pendukung apa yang dibutuhkan dalam prosedur pengelolaan hak akses dengan acuan ISO27002:2013 pada klausul A.9.2.3 Manajemen hak akses khusus yang berisikan mengenai cara melakukan pengelolaan hak akses yang benar, selain itu juga aktivitas yang dilakukan disesuaikan dengan sumber daya pada unit bisnis yang ada pada PT Angkasa Pura 1 Surabaya.

B. Prosedur Keamanan Informasi

Prosedur ini dibuat karena tidak adanya prosedur operasional secara tertulis pada instansi, prosedur ini menjelaskan langkah-langkah/aktivitas yang harus dilakukan dan dokumen pendukung apa yang dibutuhkan dalam prosedur pengelolaan hak akses dengan acuan ISO27002:2013 pada klausul A.5.1.1 Kebijakan untuk keamanan informasi dan klausul A.6.1.1 Peran dan tanggung jawab yang berisikan mengenai cara melakukan pengamanan informasi yang benar, selain itu juga aktivitas yang dilakukan disesuaikan dengan sumber daya pada unit bisnis yang ada pada PT Angkasa Pura 1 Surabaya.

C. Kebijakan keamanan informasi

Kebijakan ini dibuat berdasarkan risiko dan hasil rekomendasi pengendalian risiko yang sudah dilakukan dimana risiko yang teridentifikasi sebagai berikut:

a. Data Hilang karena kelalaian Teknisi
b. Manipulasi data karena username *password* diketahui pengguna lain.
c. Aplikasi diakses oleh tidak berwenang karena username *password* diketahui pengguna lain
d. Data tidak sesuai karena kesalahan input

Berdasarkan risiko yang dijelaskan peneliti menentukan dengan membuat kebijakan keamanan informasi yang menggunakan acuan ISO27002:2013 pada klausul A.9.4.1 Pembatasan akses informasi, A.9.4.2 Prosedur *log-on* yang aman, A.9.4.3 Sistem manajemen *password*, A.12.4.1 Pencatatan kejadian, A.12.4.2 Perlindungan informasi *log*, A.12.4.3 *Log* administrasi dan operator yang berisikan tentang pedoman pengelolaan sistem, pedoman *log-on* pada sistem, pedoman *password* pengguna, pedoman pengelolaan backup informasi, dan juga peraturan adanya *log* kegiatan pada setiap aplikasi, dan pencatatan pada setiap kegiatan, selain itu instansi juga belum memiliki dokumen kebijakan tertulis mengenai keamanan informasi. Kebijakan ini terkait dengan 2 prosedur yaitu prosedur pengelolaan *password* dan prosedur *backup* dan *restore*

D.* Prosedur pengelolaan *password

Prosedur ini dibuat karena tidak adanya prosedur operasional secara tertulis pada instansi, prosedur ini menjelaskan langkah-langkah/aktivitas yang harus dilakukan dan dokumen pendukung apa yang dibutuhkan dalam prosedur pengelolaan *password* dengan acuan ISO27002:2013 pada Klausul A.9.4.3 Sistem manajemen *password* yang berisikan mengenai tata cara dalam manajemen password, selain itu juga aktivitas yang dilakukan disesuaikan dengan sumber daya pada unit bisnis yang ada pada PT Angkasa Pura 1 Surabaya.

E.* Prosedur *backup* dan *restore

Prosedur ini dibuat karena tidak adanya prosedur operasional secara tertulis pada instansi, prosedur ini menjelaskan langkah-langkah/aktivitas yang harus

dilakukan dan dokumen pendukung apa yang dibutuhkan dalam prosedur pengelolaan *password* dengan acuan ISO27002:2013 pada A.12.3.1 *Backup* informasi yang berisikan tata cara melakukan backup data, selain itu aktivitas yang dilakukan disesuaikan dengan sumber daya pada unit bisnis yang ada pada PT Angkasa Pura 1 Surabaya.

F. **Kebijakan pengelolaan hardware dan jaringan**

Kebijakan ini dibuat berdasarkan risiko dan hasil rekomendasi pengendalian risiko yang sudah dilakukan dimana risiko yang teridentifikasi sebagai berikut:

a. Kerusakan PC karena kesalahan konfigurasi
b. Kerusakan Server karena kesalahan konfigurasi
c. Data hilang karena rusaknya media penyimpanan
d. Kerusakan kabel LAN karena kurangnya kontrol pengamanan kabel

Berdasarkan risiko yang dijelaskan peneliti menentukan dengan membuat kebijakan pengelolaan hardware dan jaringan yang menggunakan acuan ISO27002:2013 pada PT Angkasa Pura 1 Surabaya klausul A.11.2.4 Kontrol pemeliharaan peralatan,A.11.2.3 Pengendalian keamanan kabel yang berisikan tentang pedoman pengelolaan hardware dan jaringan, selain itu instansi juga belum memiliki dokumen kebijakan yang tertulis mengenai hardware dan jaringan Kebijakan ini dibuat berdasarkan risiko dan hasil rekomendasi pengendalian risiko yang sudah dilakukan dimana risiko yang teridentifikasi sebagai berikut :

a. Kerusakan PC karena kesalahan konfigurasi
b. Kerusakan Server karena kesalahan konfigurasi
c. Data hilang karena rusaknya media penyimpanan
d. Kerusakan kabel Lan karena kurangnya kontrol pengamanan kabel

Berdasarkan risiko yang dijelaskan peneliti menentukan dengan membuat kebijakan pengelolaan *hardware* dan jaringan yang menggunakan acuan ISO27002:2013 pada klausul A.11.2.4 Kontrol pemeliharaan peralatan, A.11.2.3 Pengendalian keamanan kabel yang berisikan tentang pedoman pengelolaan hardware dan jaringan, selain itu instansi juga belum memiliki dokumen kebijakan

yang tertulis mengenai *hardware* dan jaringan Kebijakan ini terkait dengan 2 prosedur yaitu prosedur perawatan *hardware* dan prosedur pengamanan kabel.

G. **Prosedur perawatan hardware**

Prosedur ini dibuat karena tidak adanya prosedur operasional secara tertulis pada instansi, prosedur ini menjelaskan langkah-langkah/aktivitas yang harus dilakukan dan dokumen pendukung apa yang dibutuhkan dalam prosedur pengelolaan *password* dengan acuan ISO27002:2013 pada Klausul A.12.3.1 *Backup* Informasi yang berisikan tata cara melakukan backup data, selain itu aktivitas yang dilakukan disesuaikan dengan sumber daya pada unit bisnis yang ada pada PT Angkasa Pura 1 Surabaya.

H. Kebijakan human *resource security*

Kebijakan ini dibuat berdasarkan risiko dan hasil rekomendasi pengendalian risiko yang sudah dilakukan dimana risiko yang teridentifikasi sebagai berikut:

a. Aplikasi diakses oleh pihak tidak berwenang karena *password* diketahui pengguna lain.
b. Data hilang karena kelalaian Teknisi
c. *Sharing password* karena kelalaian pegawai yang memiliki hak akses

Berdasarkan risiko yang dijelaskan peneliti menentukan dengan membuat *Kebijakan human resource security* yang menggunakan acuan ISO 27002:2013 pada klausul A.7.1.2. Syarat dan ketentuan kerja, A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi yang berisikan mengenai pembuatan kontrak perjanjian, dan pelatihan serta edukasi mengenai kesadaran mengenai keamanan informasi selain itu instansi juga belum memiliki dokumen kebijakan tertulis mengenai peraturan keamanan sumber daya manusia. Kebijakan ini terkait juga dengan prosedur pelatihan dan pengembangan SDM.

I. Prosedur pelatihan dan pengembangan SDM

Prosedur ini dibuat karena tidak adanya prosedur operasional secara tertulis pada instansi, prosedur ini menjelaskan langkah-langkah/aktivitas yang harus dilakukan dan dokumen pendukung apa yang dibutuhkan dalam melakukan

pelatihan dan pengembangan SDM dengan acuan ISO27002:2013 pada klausul A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi yang berisikan mengenai tata cara memberikan kesadaran dan edukasi mengenai keamanan informasi, selain itu juga aktivitas yang dilakukan disesuaikan dengan sumber daya pada unit bisnis yang ada pada PT Angkasa Pura 1 Surabaya.

4.7.3 Lanjutan Tabel Perancangan Struktur dan isi SOP

Tabel 4.7.3 - Deskripsi prosedur dan kebijakan

Struktur Bab	Sub-Bab	Konten
Pendahuluan	Tujuan	Deskripsi umum dokumen SOP Keamanan Aset Informasi
	Ruang Lingkup	
	Overview Keamanan Data	Aspek Keamanan Aset Informasi
	Evaluasi Penilaian Risiko Keamanan Aset Informasi pada PT Angkasa Pura 1 Surabaya	Tabel Daftar Prioritas Risiko Keamanan Aset Informasi
Kebijakan Pengendalian Hak Akses	Tujuan	Deskripsi umum Pengendalian Hak akses dan Keamanan Data
	Ruang lingkup	
	Referensi	Acuan yang digunakan dalam pembuatan kebijakan
Kebijakan Pengendalian Hak Akses	Rincian Kebijakan	• Pengelolaan hak akses • hak akses pihak ketiga
	Dokumen Terkait	• Prosedur pengelolaan hak akses
Kebijakan Keamanan Informasi	Tujuan	Deskripsi umum kebijakan keamanan Informasi
	Ruang Lingkup	
	Referensi	Acuan yang digunakan dalam pembuatan kebijakan
	Rincian Kebijakan	• Pengelolaan sistem informasi • Pengelolaan sistem *log-on* • *Password* pengguna • Pengelolaan *backup* dan *restore* informasi

	Dokumen Terkait	• Prosedur Pengelolaan *Password* • Prosedur *Backup* dan *Restore*
Kebijakan Pengelolaan *Hardware* dan Jaringan	Tujuan	• Deskripsi umum kebijakan pengelolaan *hardware* dan jaringan
	Ruang Lingkup	
Kebijakan Pengelolaan *Hardware* dan Jaringan	Referensi	• Acuan yang digunakan dalam pembuatan kebijakan
	Rincian Kebijakan	• Pengelolaan *hardware* • Pengelolaan jaringan
	Dokumen Terkait	• Prosedur Perawatan *Hardware* • Prosedur Pengamanan Kabel
Kebijakan *Human Resource Security*	Tujuan	• Deskripsi umum kebijakan *human resource security*
	Ruang Lingkup	
	Referensi	• Acuan yang digunakan dalam pembuatan kebijakan
	Rincian Kebijakan	• Keamanan SDM • Tanggung jawab penggunaan hak akses
	Dokumen Terkait	• Prosedur pelatihan dan pengembangan SDM
Prosedur Pengelolaan Hak Akses	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	
	Definisi	Penjelasan istilah dalam Prosedur
	Rincian Prosedur	• Proses pemberian akses • Pergantian dan penghapusan hak akses sistem aplikasi
	Bagan Alur SOP	Tabel Bagan Alur SOP
Prosedur Pengelolaan	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	
	Definisi	Penjelasan istilah dalam Prosedur

Password	Rincian Prosedur	• Proses pengelolaan *password* • Proses permintaan pergantian *password*
	Bagan Alur SOP	Tabel Bagan Alur SOP
Prosedur *Backup* dan *Restore*	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	
	Referensi	Acuan yang digunakan dalam pembuatan prosedur
	Rincian Prosedur	• Proses umum sebelum melakukan backup • Proses backup secara berkala • Proses pengujian
		• backup secara berkala • Proses *restore* data
	Bagan Alur SOP	Tabel Bagan Alur SOP
Prosedur Perawatan *Hardware*	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	
	Definisi	Penjelasan istilah dalam Prosedur
	Rincian Prosedur	• Proses pemeliharaan • Proses pemeliharaan secara keseluruhan
	Bagan Alur SOP	Tabel Bagan Alur SOP
Prosedur Keamanan Kabel	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	
	Definisi	Penjelasan istilah dalam prosedur
	Rincian Prosedur	Prosedur pengaman kabel
	Bagan Alur SOP	Tabel Bagan Alur SOP
Prosedur pelatihan dan pengembangan SDM	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	
	Definisi	Penjelasan istilah dalam prosedur
	Rincian Prosedur	• Proses pelatihan pegawai instansi • Proses pelatihan pegawai magang

	Bagan Alur SOP	Tabel Bagan Alur SOP
Prosedur Keamanan Informasi	Tujuan	Deskripsi umum SOP tentang Memberikan perlindungan aset informasi
	Ruang Lingkup	
	Definisi	Penjelasan istilah dalam Prosedur
	Rincian Prosedur	• Klasifikasi keamanan informasi • Peran dan tanggung jawab Informasi
	Bagan Alur SOP	Tabel Bagan Alur SOP
Instruksi Kerja	Instruksi Kerja Perubahan Hak Akses	
	Instruksi kerja Perubahan *password*	
	Instruksi kerja reset *password*	
	Instruksi kerja *Backup* data dan file	
	Instruksi kerja *Restore* data	
	Instruksi kerja Perawatan *Hardware*	
	Instruksi kerja Perawatan kabel jaringan telekomunikasi	
	Instruksi kerja Pelatihan dan pengembangan SDM	
	Instruksi Kerja Klasifikasi Keamanan informasi	
	Instruksi Kerja Peran dan tanggung jawab informasi	
Formulir	Form pengelolaan hak akses	
	Form kontrak perjanjian hak Akses	
	Form *log* pengelolaan hak akses	
	Form perbaikan sistem informasi	
	Form permintaan *reset password*	
	Form klasifikasi data	
	Form *log backup* data	

	Form *restore* data	
	Form pemeliharaan perangkat TI	
	Form berita acara kerusakan	
	Form laporan evaluasi pengelolaan perangkat TI	
	Form data pegawai	
	Form evaluasi kegiatan pengembangan kompetensi	
	Form Monitoring keamanan Informasi	

4.7.3 Lanjutan hasil Perencanaan SOP pada bagian kebijakan (point 1)

a. **Kebijakan pengendalian hak akses**

Sesuai dengan kontrol dalam ISO27002:2013 sub klausul *9.1.1* Kebijakan pengendalian kontrol akses, *12.4.1* Pencatatan kejadian, dalam kebijakan ini terdapat beberapa hal yang terkandung di dalamnya yang mengatur mengenai pengelolaan hak akses. terlampir pada Lampiran 7 hasil perancangan kebijakan (KB 01. Kebijakan pengendalian hak akses).

b. Kebijakan keamanan informasi

Sesuai dalam kontrol ISO 27002:2013 pada klausul 9.4.1 Pembatasan akses informasi, *5.1.1* Kebijakan untuk keamanan informasi, 6.1.1 Peran dan tanggung jawab, *9.4.2* Prosedur *log-on* yang aman, *9.4.3* Sistem manajemen *password* ,*12.3.1 Backup* informasi,*12.4.1* Pencatatan kejadian,*12.4.2* Perlindungan informasi *log,* dalam kebijakan memuat peraturan untuk menjamin keamanan dari informasi penting baik informasi digital dan fisik yang dimiliki instansi, terlampir pada Lampiran 7 hasil perancangan kebijakan (KB 02. Kebijakan keamanan informasi).

c. **Kebijakan pengelolaan *hardware* dan jaringan**

Sesuai dalam kontrol ISO 27002:2013 pada klausul *11.2.3* Pengendalian keamanan kabel dan *11.2.4.* Kontrol pemeliharaan peralatan dalam kebijakan memuat peraturan untuk menjamin fasilitas perangkat hardware dan jaringan agar dapat selalu beroperasi selama proses bisnis berlangsung, terlampir pada Lampiran 7 hasil perancangan kebijakan (KB 03. Kebijakan pengelolaan *hardware* dan

jaringan).

d. **Kebijakan *human resource security***

Sesuai dalam kontrol ISO 27002:2013 pada klausul *7.1.2.* Syarat dan ketentuan kerja, *7.2.2.* Kepedulian, pendidikan dan pelatihan keamanan informasi, *9.3.1.* Penggunaan informasi autentikasi rahasia dalam kebijakan memuat peraturan kepada seluruh civitas instansi dalam memberi perlindungan keamanan pada aset informasi yang dimiliki instansi, terlampir pada Lampiran 7 hasil perancangan kebijakan (KB 04. Kebijakan *human resource security*).

4.7.3 Lanjutan hasil Perencanaan SOP pada bagian prosedur (point 2)

1. Hasil Perancangan Prosedur

Hasil perancangan instruksi kerja dalam mendukung pelaksanaan SOP, dibutuhkan beberapa prosedur dengan tujuan mendokumentasikan dengan baik setiap aktivitas. Berikut adalah 7 prosedur yang dibutuhkan untuk mendukung pelaksanaan SOP yaitu sebagai berikut.

a. Prosedur Pengelolaan Hak Akses

Prosedur pengelolaan hak akses merupakan prosedur untuk menjadi pedoman dalam memberikan alokasi dan penggunaan hak akses terhadap sistem informasi yang seharusnya dikontrol dalam rangka melindungi keamanan data baik dari dalam maupun luar lingkungan instansi Terlampir pada Lampiran 8 hasil perancangan prosedur (PO 01. Prosedur pengelolaan hak akses).

b. **Prosedur Pengelolaan *Password***

Prosedur Manajemen *password* merupakan prosedur untuk memastikan pengelolaan penggunaan *password* telah memenuhi kualitas standar *strong password* dan memastikan *password* setiap pengguna telah sesuai dengan syarat kualitas password terlampir pada Lampiran 8 hasil perancangan prosedur (PO 02. Prosedur pengelolaan *password*).

c. Prosedur Backup dan Restore

Prosedur ini menjelaskan langkah-langkah dalam aktivitas *backup* yang sesuai dengan kontrol ISO27001:2013, sub klausul 12.3.1 *backup* informasi. Prosedur *Back up* dan *restore* dibagi kedalam empat proses utama yang terdiri dari

beberapa aktivitas yang berurutan. Namun, sebelum mendeskripsikan prosedur penanganan secara terstruktur, terlebih dahulu didefinisikan informasi pendukung yang dibutuhkan untuk menunjang aktivitas didalam prosedur tersebut. Pendefinisian tersebut berguna untuk menentukan strategi *back up* yang sesuai dengan kebutuhan bisnis Pendefinisian dalam prosedur *Backup* dibagi kedalam tiga yaitu pendefinisian klasifikasi data, pendefinisian kritikalitas data dan pendefinisian tipe *back up*, terlampir pada Lampiran 8 hasil perancangan prosedur (PO 03. Prosedur *backup* dan *restore*).

d. **Prosedur Pengelolaan *Hardware***

Prosedur pengelolaan *hardware* ini merupakan pedoman dan acuan untuk melakukan pengelolaan aset *hardware* pada instansi baik dalam melakukan pengadaan barang, maintenance, penggunaan serta keamanan dari *hardware* itu sendiri terlampir pada Lampiran 8 hasil perancangan prosedur (PO 04 Prosedur pengelolaan *hardware*).

e. Prosedur Prosedur pengelolaan kabel jaringan telekomunikasi

Prosedur Prosedur pengelolaan kabel jaringan telekomunikasi merupakan prosedur yang berguna untuk memastikan bahwa seluruh kabel telekomunikasi yang membawa data dan mendukung layanan informasi pada instansi diatur atau dikelola secara terstruktur sehingga terlindungi dari kerusakan, terlampir pada Lampiran 8 hasil perancangan prosedur (PO 05. Prosedur pengelolaan kabel jaringan telekomunikasi).

f. Prosedur Pelatihan dan Pengembangan SDM

Prosedur pelatihan dan pengembangan SDM merupakan prosedur yang mengatur segala pelatihan atau edukasi terkait keamanan informasi untuk pegawai yang mampu meningkatkan kualitas baik secara intelektual maupun kepribadian, sehingga mampu menjaga aset informasi yang dimiliki oleh instansi, terlampir pada Lampiran 8 hasil perancangan prosedur (PO 06. Prosedur pelatihan dan pengembangan SDM).

g. Prosedur Keamanan Informasi

Prosedur keamanan informasi merupakan prosedur yang berguna untuk

memastikan bahwa seluruh aset informasi pada instansi diatur dan dikelola secara terstruktur sehingga terlindungi dari kerusakan, terlampir pada Lampiran 8 hasil perancangan prosedur (PO 07. Prosedur pengelolaan keamanan informasi).

4.7.3 Lanjutan hasil Perencanaan SOP pada bagian instruksi kerja (point 3)

2. Hasil Perancangan Instruksi Kerja

Hasil perancangan instruksi kerja dalam mendukung pelaksanaan SOP, dibutuhkan beberapa formulir dengan tujuan mendokumentasikan dengan baik setiap aktivitas. Berikut adalah 10 instruksi kerja yang dibutuhkan untuk mendukung pelaksanaan SOP yaitu sebagai berikut.

a. Instruksi kerja Pengelolaan hak akses

Dalam dokumen prosedur pemberian hak akses dibutuhkan sebuah instruksi kerja yaitu instruksi dalam melakukan pemberian hak akses yang bertujuan untuk membantu pegawai baru untuk mengakses sistem informasi yang diizinkan. Terlampir pada Lampiran 9 Hasil perancangan instruksi kerja (IK 01. Instruksi kerja pengelolaan hak akses).

b. **Instruksi kerja Perubahan *password***

Dalam dokumen prosedur perubahan *password* dibutuhkan sebuah instruksi kerja yaitu instruksi dalam melakukan perubahan *password* yang bertujuan untuk membantu pegawai dalam melakukan perubahan *password* baik pegawai baru ataupun pegawai tetap. Terlampir pada Lampiran 9 Hasil perancangan instruksi kerja (IK 02. Instruksi kerja perubahan password).

c. **Instruksi kerja *reset password***

Dalam dokumen Prosedur pengelolaan *password*, juga dibutuhkan sebuah instruksi kerja yaitu instruksi kerja reset *password* yang bertujuan untuk membantu kerja pegawai baru dalam mempelajari proses reset *password*, terlampir pada Lampiran 9 Hasil perancangan instruksi kerja (IK 03. Instruksi kerja *reset password*).

d. Instruksi kerja backup data dan file

Dalam dokumen Prosedur *Backup* dan R*estore* dibutuhkan sebuah instruksi

kerja yaitu instruksi kerja *back up* yang bertujuan untuk membantu kerja ICT dalam mempelajari proses *backup* data maupun *backup file*, terlampir pada Lampiran 9. Hasil perancangan instruksi kerja (IK 04 Instruksi kerja *backup* data dan *file*).

e. Instruksi kerja *restore* data

Dalam dokumen Prosedur *Backup* dan *Restore*, juga dibutuhkan sebuah instruksi kerja yaitu instruksi kerja *restore* yang bertujuan untuk membantu kerja DB Teknisi baru dalam mempelajari proses *restore*, terlampir pada Lampiran 9 Hasil perancangan instruksi kerja (IK 05. Instruksi kerja *restore* data).

f. Instruksi kerja perawatan hardware

Dalam dokumen Prosedur pengelolaan *password*, juga dibutuhkan sebuah instruksi kerja yaitu instruksi kerja perawatan *hardware* yang bertujuan untuk membantu kerja pegawai baru dalam mempelajari proses perawatan *hardware*, terlampir pada Lampiran 9 Hasil perancangan instruksi kerja (IK 06. Instruksi kerja perawatan *hardware)*.

g. Instruksi kerja perawatan kabel jaringan telekomunikasi

Dalam dokumen Prosedur pengelolaan *password*, juga dibutuhkan sebuah instruksi kerja yaitu instruksi kerja perawatan kabel yang bertujuan untuk membantu kerja pegawai baru dalam mempelajari proses perawatan kabel, terlampir pada Lampiran 9 Hasil perancangan instruksi kerja (IK 07. Instruksi kerja perawatan kabel jaringan telekomunikasi).

h. Instruksi kerja pelatihan dan pengembangan SDM

Dalam dokumen Prosedur pengelolaan *password*, juga dibutuhkan sebuah instruksi kerja yaitu instruksi kerja pelatihan dan pengembangan SDM instansi yang bertujuan untuk membantu kerja pegawai baru dalam proses pelatihan dan pengembangan SDM instansi terlampir pada Lampiran 9 Hasil perancangan instruksi kerja (IK 08. Instruksi kerja pelatihan dan pengembangan SDM).

i. Instruksi Kerja Klasifikasi Keamanan informasi

Dalam dokumen Prosedur keamanan informasi, juga dibutuhkan sebuah instruksi kerja yaitu instruksi kerja klasifikasi keamanan informasi yang bertujuan

untuk membantu dalam mengklasifikasikan informasi yang ada dalam instansi. terlampir pada Lampiran 9 Hasil perancangan instruksi kerja (IK 09. Instruksi kerja klasifikasi keamanan informasi).

j. Instruksi Kerja peran dan tanggung jawab informasi

Dalam dokumen Prosedur keamanan informasi, juga dibutuhkan sebuah instruksi kerja yaitu instruksi kerja peran dan tanggung jawab informasi yang bertujuan untuk membantu kerja pegawai dalam memahami peran dan tanggung jawab dalam penyampaian informasi instansi. terlampir pada Lampiran 9 Hasil perancangan instruksi kerja (IK 10. Instruksi kerja peran dan tanggung jawab informasi).

4.7.3 Lanjutan hasil Perencanaan SOP pada bagian rekam kerja (point 4)

3. Hasil Perancangan Formulir

Hasil perancangan formulir dalam mendukung pelaksanaan SOP dibutuhkan beberapa formulir dengan tujuan mendokumentasikan dengan baik setiap aktivitas. Berikut adalah 14 formulir yang dibutuhkan untuk mendukung pelaksanaan SOP yaitu sebagai berikut.

a. Formulir Pengelolaan hak akses

Formulir pengelolaan hak akses adalah formulir yang digunakan dalam prosedur pengelolaan hak akses dimana formulir ini berguna untuk mendokumentasikan pemberian hak akses pada pengguna sistem untuk dilakukan persetujuan pada pihak manajemen Terlampir pada Lampiran 10 Hasil perancangan formulir (FM 01. Formulir pengelolaan hak akses).

b. Formulir kontrak perjanjian hak akses

Formulir kontrak perjanjian hak akses adalah formulir yang digunakan dalam prosedur pengelolaan hak akses yang berfungsi sebagai sebuah peraturan dan tanggung jawab yang harus disetujui oleh pengguna sistem jika hak akses diberikan terlampir pada Lampiran 10 Hasil perancangan formulir (FM 02. Formulir kontrak perjanjian hak akses).

c. Formulir *log* pengelolaan hak akses

Formulir *log* pengelolaan hak akses adalah formulir yang berfungsi sebagai

media pencatatan pemberian, penghapusan ataupun pergantian hak akses yang dilakukan terlampir pada Lampiran 10 Hasil perancangan formulir (FM 03. Formulir *log* pengelolaan hak akses).

d. Formulir perbaikan system informasi

Formulir perbaikan system informasi adalah formulir yang digunakan untuk melakukan perbaikan pada sistem informasi atau aplikasi yang dimiliki instansi, terlampir pada Lampiran 10 Hasil perancangan formulir (FM 04. Formulir perbaikan system informasi).

e. **Formulir permintaan *reset password***

Formulir permintaan pergantian *password* adalah formulir yang digunakan untuk prosedur pergantian *password* sebelum meminta pergantian *password* pengguna harus mengisi formulir ini, terlampir pada Lampiran 10 Hasil perancangan formulir (FM 05. Formulir permintaan *reset password).*

f. Formulir klasifikasi data

Formulir klasifikasi data digunakan untuk menentukan strategi *back-up* yang digunakan. Berdasarkan kontrol dalam ISO27001:2013, penentuan strategi *back up* data ditentukan sesuai dengan kebutuhan bisnis organisasi dilihat dari kebutuhan keamanan dan tingkat kritikalitas data. Klasifikasi data didasarkan pada tingkat sensitivitas data dan tingkat kritikalitas data terlampir pada Lampiran 10 Hasil perancangan formulir (FM 06. Formulir klasifikasi data).

g. Formulir *log backup* data

Formulir *log back up* digunakan oleh DB Teknisi untuk melakukan pemantauan (*monitoring*) secara berkala pada hasil eksekusi *back up* data. Tujuan dari formulir log back up data ini adalah untuk memastikan bahwa hasil eksekusi *backup* data telah akurat dan lengkap dan juga untuk memastikan keberhasilan data yang ter-*back up* dan data yang tidak berhasil *di-back up*, terlampir pada Lampiran 10 Hasil perancangan formulir (FM 07. Formulir *log backup* data).

h. Formulir *restore* data

Formulir restore digunakan untuk permintaan kebutuhan *restore* data oleh pihak tertentu/unit kerja tertentu. Formulir *restore* data dibutuhkan untuk menjaga integritas data dan memastikan bahwa setiap proses *restore* data terdokumentasi dengan baik dan telah divalidasi oleh pegawai bagian personalia yang bertanggung

jawab, terlampir pada Lampiran 10 Hasil perancangan formulir (FM 8. Formulir *restore* data).

i. Formulir pemeliharaan perangkat TI

Formulir pemeliharaan perangkat TI adalah formulir yang digunakan untuk melakukan pencatatan kegiatan (*log*) dalam melakukan perbaikan perangkat TI yang dimiliki instansi terlampir pada Lampiran 10 Hasil perancangan formulir (FM 09. Formulir pemeliharaan perangkat TI).

j. Formulir berita acara kerusakan

Formulir berita acara kerusakan adalah formulir yang digunakan untuk pelaporan kerusakan pada perangkat TI yang dimiliki instansi, terlampir pada Lampiran 10 Hasil perancangan formulir (FM 10. Formulir berita acara kerusakan).

k. Formulir laporan evaluasi pengelolaan perangkat TI

Formulir laporan evaluasi adalah formulir yang digunakan dalam pencatatan setiap kegiatan pengelolaan perangkat TI baik itu perbaikan secara parsial maupun keseluruhan yang dilakukan, terlampir pada Lampiran 10 Hasil perancangan formulir (FM 11. Formulir laporan evaluasi pengelolaan perangkat TI).

l. Formulir data pegawai

Formulir data pegawai adalah formulir yang digunakan instansi dalam prosedur pelatihan dan pengembangan SDM untuk mencatat pegawai yang mengikuti program pelatihan yang diadakan instansi terkait dengan keamanan aset informasi, terlampir pada Lampiran 10 Hasil perancangan formulir (FM 12. Formulir data pegawai).

m. Formulir evaluasi kegiatan pengembangan kompetensi.

Formulir evaluasi kegiatan pengembangan kompetensi adalah formulir digunakan untuk melakukan evaluasi pelatihan maupun pengembangan pegawai yang dilakukan instansi, terlampir pada Lampiran 10 Hasil perancangan formulir (FM 13. Formulir pengelolaan evaluasi kegiatan pengembangan kompetensi).

n. Formulir Monitoring keamanan informasi

Formulir Monitoring keamanan informasi adalah formulir digunakan untuk melakukan monitoring keamanan informasi guna mengetahui informasi apa yang

disampaikan. terlampir pada Lampiran 10 Hasil perancangan formulir (FM 14. Formulir Monitoring keamanan informasi).

LAMPIRAN 9

MAPPING SOLUSI, KLAUSUL, DAN KONTROL OBJEKTIF

PERMASALAHAN	PENYEBAB	DAMPAK	ALTERNATIF SOLUSI
- Tidak adanya kebijakan keamanan informasi yang dikomunikasikan ke semua staff - Belum adanya kebijakan peran dan tanggung jawab keamanan informasi - Tidak ada aturan tentang keamanan *transfer* informasi	Kurangnya kebijakan SMKI	Kehilangan atau kerusakan informasi terkait perencanaan pengadaan alat bagasi	- Membuat dokumen kebijakan keamanan informasi - Membuat dokumen Organisasi keamanan Informasi - Membuat dokumen Keamanan Operasi
- Belum adanya kebijakan hak akses terhadap penggunaan informasi terkait perencanaan pengadaan barang - Tidak adanya kebijakan keamanan informasi	Belum adanya kebijakan informasi (autent dan Autorisasi)	Tidak tersedianya informasi perencanaan pengadaan fasilitas bandara	- Membuat dokumen kebijakan keamanan informasi - Membuat dokumen kebijakan informasi (Autentikasi dan Autorisasi) terkait Kontrol Akses
- tidak adanya kebijakan keamanan informasi yang dikomunikasikan ke semua staff - Belum adanya kebijakan akses kontrol untuk penggunaan aplikasi FIDS - Kurangnya kebijakan manajemen insiden	Belum adanya kebijakan informasi (autentikasi dan Autorisasi)	- Kondisi saat ini pernah terjadi kehilangan informasi jadwal penerbangan. - Rusak atau hilangnya data maskapai	- Membuat dokumen kebijakan keamanan informasi - Membuat dokumen kebijakan informasi (Autentikasi dan Autorisasi) terkait Kontrol Akses - Membuat dokumen informasi manajemen insiden - Membuat dokumen keamanan fisik dan lingkungan

- kurangnya kebijakan tentang lingkungan sekitar penyimpanan informasi penting - belum adanya manajemen asset terkait data maskapai			- Membuat dokumen manajemen asset
- Belum adanya manajemen penerapan keamanan informasi pada organisasi - Belum adanya kebijakan tanggung jawab tiap sumber daya manusianya terkait keamanan informasi	Belum adanya kebijakan SMKI	- Tidak tersedianya informasi jadwal shift kerja pegawai - Tidak tersedianya informasi operator garbarata	- Membuat dokumen Organisasi Keamanan Informasi - Membuat dokumen Keamanan Sumber Daya Manusia
- Kurangnya kebijakan manajemen aset informasi - Ketika transfer data atau informasi hanya melalui email yang tidak terenkripsi - Belum adanya evaluasi keamanan informasi secara kontinuitas	Kurangnya kebijakan SMKI	Hilang atau rusaknya informasi terkait hasil evaluasi tiap layanan bisnis utama	- Membuat dokumen manajemen asset - Membuat dokumen kriptografi - Membuat dokumen aspek keamanan informasi manajemen kelangsungan bisnis

LAMPIRAN 10

PEMETAAN HASIL REKOMENDASI PENGENDALIAN RISIKO

Kontrol ISO 27002:2013	Kontrol Objektif	Petunjuk Pelaksanaan	Pelaksanaan Keamanan yang dilakukan Instansi	Hasil Rekomendasi
A.5.1.1 Kebijakan untuk keamanan informasi	Untuk memberikan arahan manajemen dan dukungan untuk keamanan informasi sesuai dengan persyaratan bisnis dan hukum dan peraturan yang relevan	• Kebijakan keamanan informasi harus memenuhi persyaratan yang dibuat oleh: a) Strategis bisnis b) Peraturan perundang-undangan dan kontrak c) Lingkungan ancaman keamanan informasi saat ini yang di proyeksikan.	• Instansi memberikan tanggung jawab keamanan informasi yang dikelola untuk masing-masing pegawai sesuai dengan unti kerja dan fungsinya.	• Membuat kontrak perjanjian untuk semua pegawai yang diberikan tanggung jawab dan hak akses pada pengelolaan informasi • Adanya tanggung jawab secara hukum untuk pegawai yang menandatangani perjanjian perihal perlindungan informasi.
A.6.1.1 Peran dan tanggung jawab	Untuk membangun kerangka kerja manajemen untuk memulai dan mengendalikan	• Area yang menjadi tanggung jawab individu harus dinyatakan. Khususnya hal-hal berikut harus terjadi: a) Asset dan proses keamanan informasi harus diidentifikasikan dan didefinisikan; b) Entitas yang bertanggung jawab untuk setiap asset atau proses	• Instansi memberikan tanggung jawab keamanan informasi yang dikelola untuk masing-masing pegawai sesuai dengan unit kerja dan fungsinya	• Membuat kontrak perjanjian untuk semua pegawai yang diberikan tanggung jawab dan hak akses pada pengelolaan informasi • Adanya tanggung jawab secara hukum untuk pegawai yang menandatangani perjanjian perihal perlindungan informasi

		keamanan informasi harus ditugaskan dan rincian tanggung jawab ini harus didokumentasikan (lihat 8.1.2) c) Tingkat otorisasi harus didefinisikan dan didokumentasikan d) Untuk dapat memenuhi tanggung jawab di bidang keamanan informasi, individu yang ditunjuk harus kompeten di area tersebut dan diberi kesempatan untuk mengikuti perkembangan terkini e) Koordinasi dan pengawasan aspek keamanan informasi		
A.7.1.2 syarat dan ketentuan kerja	Perjanjian kontrak dengan pegawai yang menyatakan bahwa mereka bertanggung jawab atas keamanan informasi instansi	• Semua pegawai yang diberikan akses informasi rahasia harus menandatangani perjanjian *non-disclosure* sebelum diberi akses pada pengelolaan informasi	• Instansi memberikan tanggung jawab hak akses yang dikelola untuk masing-masing pegawai sesuai dengan unit kerja dan fungsinya • Instansi memberlakukan punishment terhadap pegawai yang melanggar	• Membuat kontrak perjanjian untuk semua pegawai yang diberikan tanggung jawab dan hak akses pada pengelolaan informasi • Adanya tanggung jawab secara hukum untuk

		• Adanya tanggung jawab hukum untuk hak dari pegawai, misalnya hak cipta atau undang-undang perlindungan data • Adanya tanggung jawab untuk klasifikasi informasi dan manajemen asset instansi terkait dengan informasi, fasilitas pengelolaan informasi dan layanan informasi yang ditangani oleh pegawai • Adanya tanggung jawab pegawai untuk penanganan informasi yang diterima dari instansi lain atau untuk pihak eksternal • Adanya Tindakan yang harus diambil jika pegawai atau mengabaikan persyaratan keamanan organisasi	peraturan hak akses seperti pengurangan gaji dan pergantian hak akses	pegawai yang menandatangani perjanjian perihal perlindungan informasi. • Adanya tanggung jawab untuk klasifikasi informasi dan manajemen asset instansi terkait dengan informasi, fasilitas pengelolaan informasi dan layanan informasi yang ditangani oleh pegawai • Adanya tanggung jawab pegawai untuk penanganan informasi yang diterima dari instansi lain atau untuk pihak eksternal • Adanya Tindakan yang harus diambil jika pegawai atau mengabaikan persyaratan keamanan organisasi
A.7.2.2 Kepedulian Pendidikan dan pelatihan keamanan informasi	Semua pegawai harus memiliki kesadaran, edukasi, dan pelatihan terkait kebijakan dan prosedur instansi sesuai dengan fungsi kerja mereka	• Program *awareness* (peringatan kesadaran) terkait keamanan informasi membuat para pegawai menyadari tanggung jawab mereka untuk keamanan informasi instansi dan	• Adanya pemberitahuan dan peringatan setiap pegawai saat diberikan tanggung jawab hak akses maupun tugas agar mengerjakan dengan teliti dan benar	• Membuat program kesadaran training dan seminar secara terjadwal untuk setiap pegawai yang menggunakan asset informasi baik pegawai baru, pegawai lama, dan

		supaya mereka tidak mengabaikannya • Program *awareness* (peringatan kesadaran) terkait keamanan informasi harus ditetapkan sesuai dengan kebijakan dan prosedur instansi	• Adanya pemberitahuan dan peringatan setiap pegawai mengenai betapa pentingnya data yang dikerjakan maupun yang berada dibawah tanggung jawabnya. • Adanya training setiap adanya *software* baru maupun *update software*	pegawai sementara atau magang • Membuat poster mengenai kesadaran keamanan informasi pada setiap bagian instansi yang menggunakan asset informasi. • Membuat perencanaan dan konten program kesadaran yang sesuai dengan kebutuhan dengan mempertimbangkan peran dari pegawai
		• Program *awareness* (peringatan kesadaran) harus direncanakan dengan mempertimbangkan peran pegawai dalam organisasi. Kegiatan ini harus dijadwalkan dari waktu ke waktu secara teratur sehingga kegiatan ini mampu diikuti oleh pegawai yang baru. Program ini juga harus diperbarui secara berkala sehingga tetap sejalan dengan kebijakan dan prosedur organisasi, dan juga dapat diperbarui dari	• Adanya training untuk pegawai magang ataupun pegawai baru	• Membuat reward dan punishment untuk pegawai yang menjalankan program kesadaran dengan sesuai

		insiden keamanan informasi yang pernah terjadi • Program *awareness* harus dilakukan sesuai kebutuhan keamanan informasi organisasi. *Awareness* training dapat menggunakan media pengiriman yang berbeda, pembelajaran jarak jauh, berbasis *website, self-paced learning,* dan lain-lain.		
A.9.1.1 Kebijakan pengendalian kontrol akses	Kebijakan untuk mengontrol hak akses harus ditetapkan, didokumentasikan dan ditinjau berdasarkan bisnis dan kebutuhan keamanan informasi instansi	• Pengguna dan penyedia layanan harus diberikan pernyataan yang jelas dari kebijakan kontrol akses memperhatikan hal-hal berikut: • Kebutuhan keamanan dari aplikasi • Kebijakan untuk penyebaran informasi dan otorisasi • Konsistensi antara hak akses dan kebijakan klasifikasi informasi dari sistem dan jaringan; • Peraturan yang relevan dan kewajiban kontraktual mengenai	• Instansi memiliki catatan *log* setiap aktivitas dalam sistem informasi yang dimiliki misalkan *log login* siapa saja yang akses aplikasi, apa saja data yang baru dimasukkan, di ubah, maupun dihapus • Instansi membedakan role atau hak akses untuk masing-masing pegawai sesuai dengan unit kerja dan fungsinya • Setiap *system* memiliki user level, direktur, kepala bagian dan staff memiliki *user interface* yang berbeda	• Membuat aturan yang jelas dan tertulis mengenai hak akses terhadap asset sistem informasi yang di dalamnya ada antara lain: ○ Kebutuhan keamanan dari aplikasi ○ Peraturan kebijakan untuk penyebaran informasi ○ Peraturan relevan dan kebijakan secara tertulis atau kontraktual mengenai pembatasan akses

		pembatasan akses data atau layanan • Pengelolaan hak akses dalam lingkungan terdistribusi dan jaringan yang mengakui semua jenis koneksi yang tersedia • Pemisahan peran kontrol akses • Requirement untuk otorisasi permintaan akses • Requirement untuk mereview hak akses • Penghapusan hak akses • Pengarsipan catatan semua peristiwa penting mengenai penggunaan dan pengelolaan identitas pengguna dan informasi autentikasi rahasia • *Roles* terkait *privilege* akses	• Instansi memberlakukan peraturan tidak dapat menginstall aplikasi lain dalam PC selain admin yang ada pada instansi hanya berisikan aplikasi-aplikasi yang menunjang kinerja instansi • Data instansi hanya bisa dimasukkan, diganti atau terhapus oleh *database* teknisi saja, sehingga para staf tidak dapat memodifikasi data yang sifatnya rahasia	○ Peraturan pengelolaan hak akses, penghapusan serta *roles* yang diberikan ○ Pengarsipan catatan semua kegiatan mengenai penggunaan dan pengelolaan • Membuat peraturan mengenai pembatasan akses data manapun sistem aplikasi yang dimiliki: ○ Pemisahan peran kontrol akses ○ Roles terkait *privileged* akses ○ *Requirement* otorisasi hak akses ○ *Requirement mereview* hak akses
A.9.2.3 Manajemen Hak akses	Alokasi dan penggunaan hak akses *privileges* harus dibatasi dan di kontrol	• Hak akses *privileges* yang terkait dengan setiap system atau proses (ex. System manajemen database dan masing-masing aplikasi dan pengguna operasi kepada siapa mereka harus	• Instansi telah membedakan role atau hak akses untuk masing-masing pegawai sesuai dengan unit kerja dan fungsinya ○ Setiap sistem memiliki user level, direktur, kepala	• Adanya membedakan *role* atau hak akses masing-masing pegawai sesuai dengan unit kerja dan fungsinya • Membuat aturan prosedur tertulis mengenai penggunaan hak akses *privileges*

		dialokasikan harus diidentifikasikan) • Hak akses *privileged* harus dialokasikan kepada pengguna berdasarkan kebutuhan yang digunakan dan sejalan dengan kebijakan kontrol akses • Proses otorisasi dan catatan hak *privileged* yang dialokasikan harus didokumentasikan kebutuhan untuk hak akses *privileged* harus didefinisikan • Hak akses *privileged* harus diserahkan kepada pengguna ID yang berbeda dari yang digunakan untuk kegiatan bisnis biasa • Kompetensi pengguna dengan hak akses *privileged* harus ditinjau secara teratur untuk memverifikasi apakah mereka sejalan dengan tugas mereka • Prosedur tertentu harus ditetapkan dan di *maintenance* untuk menghindari penggunaan	bagian, dan staf memiliki user *interface* yang berbeda ○ Data instansi hanya bisa dimasukkan, diganti atau dihapus oleh *database* teknis saja. Sehingga para staf tidak dapat memodifikasi data yang sifatnya rahasia • adanya prosedur yang telah berjalan untuk melakukan pergantian *password* ○ Setiap 3 bulan sekaIi system secara otomatis meminta teknisi untuk melakukan perubahan *password*	○ Proses otorisasi dan catatan hak *privileged* yang dialokasikan harus didokumentasikan ○ Kebutuhan untuk hak akses *privileged* harus didefinisikan ○ Peninjauan pengguna atau hak akses *privileged* harus diserahkan kepada pengguna ID yang berbeda dari yang digunakan untuk kegiatan bisnis dengan yang biasa pegawai yang diberikan hak akses secara teratur untuk memverifikasi apakah sudah sesuai dengan tugas yang di berikan ○ Adanya autentikasi rahasia dari ID administrasi maupun pemilik hak akses seperti sering mengubah *password* dan *log-out* sesegera mungkin Ketika pengguna hak *privileged*

		yang tidak sah dari ID pengguna • Untuk ID administrasi, pengguna *generic*, kerahasiaan informasi autentikasi rahasia harus dijaga saat Bersama (ex. Sering mengubah *password* dan menghapus segera mungkin Ketika penggunaan hak akses • *Privileged* meninggalkan atau mengubah pekerjaan)		meninggalkan atau mengubah pekerjaan.
A.9.3.1 Penggunaan informasi autentikasi rahasia	Pengguna harus diminta untuk mengikuti praktek-praktek organisasi dalam penggunaan informasi autentikasi rahasia	• Menyimpan autentikasi informasi rahasia, memastikan bahwa tidak dibocorkan kepada pihak lain • Menjaga kerahasiaan catatan autentikasi informasi • Mengubah autentikasi informasi rahasia setiap kali ada indikasi masalah yang mungkin terjadi • Ketika *password* digunakan sebagai autentikasi informasi rahasia, pilih *password* yang berkualitas dengan Panjang minimum 8 dan bebas karakter yang	• Instansi telah membedakan role atau hak akses untuk masing-masing pegawai sesuai dengan unit kerja dan fungsinya ○ Setiap system memiliki user level, direktur, kepala bagian, dan staf memiliki user *interface* yang berbeda • Adanya prosedur yang telah berjalan untuk melakukan pergantian *password* ○ Setiap 3 bulan sekaIi system secara	• Adanya penyimpanan autentikasi rahasia khusus untuk memastikan bahwa dokumen tidak dibocorkan kepada pihak lain • Mengubah autentikasi informasi rahasia setiap terjadinya indikasi masalah • Diharuskan menggunakan *password* yang berkualitas dengan Panjang minimum 8 dan *alphanumeric* • Tidak membagikan autentikasi rahasia dengan individu lain

		identik (semua abjad atau semua angka) • Tidak berbagi autentikasi informasi rahasia dengan individu lain • Memastikan perlindungan yang tepat dari *password* Ketika *password* yang digunakan sebagai informasi autentikasi rahasia otomatis *log-on* disimpan	otomatis meminta teknisi untuk melakukan perubahan *password* • Adanya pemberitahuan dan peringatan setiap pegawai mengenai betapa pentingnya data yang dikerjakan maupun yang berada di bawah tanggung jawabnya	• Adanya pemastian *password* yang digunakan adalah strong dan keamanan penyimpanan di password aman. • Tidak menggunakan informasi autentikasi yang sama untuk tujuan bisnis dan *non-bisnis*.
A.9.4.3 Pembatasan Akses Informasi	Akses untuk fungsi informasi dan system aplikasi harus dibatasi sesuai dengan kebijakan kontrol akses	• Menyediakan menu untuk kontrol akses ke fungsi system aplikasi • Pengendalian data yang dapat diakses oleh pengguna tertentu • Mengontrol hak akses pengguna (Ex, read, create, delete dan execute) • Mengontrol hak akses dari aplikasi lain membatasi informasi yang terkandung dalam output • Menyediakan kontrol akses fisik atau logika untuk isolasi aplikasi sensitif, aplikasi data, atau sistem.	• Instansi telah membedakan *role* atau hak akses untuk masing-masing pegawai sesuai dengan unit kerja dan fungsinya ○ Setiap system memiliki user level, direktur, kepala bagian, dan staf memiliki user *interface* yang berbeda • Data instansi hanya bisa dimasukkan, diganti atau dihapus oleh *database* teknisi saja ○ Sehingga para staf tidak dapat memodifikasi data	• Adanya men khusus pada sistem aplikasi untuk mengubah kontrol akses yang ada • Adanya pengendalian data yang dapat diakses oleh pengguna tertentu • Mengontrol penyesuaian pengguna hak akses oleh pengguna (*Ex. Read, create, delete, and execute*) pada sistem aplikasi • Membedakan hak akses dari aplikasi lain • Adanya kontrol akses fisik atau logika untuk isolasi aplikasi sensitif, aplikasi data atau sistem (*Ex. Camera CCTV,*

			yang sifatnya confidential • Instansi memberlakukan peraturan tidak menginstal aplikasi lain dalam PC selain admin ○ PC yang ada di instansi hanya berisikan aplikasi-aplikasi yang menunjang kinerja instansi	penggembokan ruangan, dll)
A.9.4.2 Prosedur *log-on* yang aman	Akses ke system dan aplikasi harus dikontrol dengan prosedur keamanan *log-on*	• Tidak menampilkan system atau aplikasi pengenal hingga proses *log-on* terselesaikan • Menampilkan pemberitahuan umum yang memperingatkan bahwa computer hanya bisa akses oleh pengguna yang berwenang • Tidak memberikan bangunan pesan selama proses *log-on* memvalidasi *log-on* hanya pada proses input data terselesaikan. Jika ada kesalahan, system tidak harus menunjukkan bagaimana data yang benar *brute force log-on* • Percobaan *log unsuccess* dan log *success*	• Adanya autentikasi untuk login pengguna ○ Setiap menggunakan system yang ada pada instansi, pengguna harus memasukkan *username* dan *password* ang sesuai terlebih dahulu • Data instansi hanya bisa dimasukkan, diganti atau dihapus oleh *database* teknisi saja. Sehingga para staf tidak dapat memodifikasi data yang sifatnya rahasia • Instansi memiliki catatan *log* setiap aktivitas dalam sistem informasi yang dimiliki misalkan *log login* siapa saja yang	• Adanya proses *log-on* pada setiap sistem aplikasi • Adanya notifikasi yang memperingatkan sistem aplikasi hanya dapat diakses oleh pengguna yang berwenang • Tidak adanya hint atau bantuan dalam proses *log-on* sehingga hanya dapat diakses oleh pihak yang berwenang saja • Tidak adanya pemberitahuan penulisan input data yang benar selama proses log-on • Adanya perlindungan terhadap *brute force* • Meningkatkan keamanan jika terjadi potensi

		• Meningkatkan keamanan jika terdapat potensi pelanggaran yang terdeteksi
		• Menampilkan informasi berikut pada proses *log-on* selesai:
		  ○ Tanggal dan waktu dari sukses *log-on* sebelumnya
		  ○ Rincian dari setiap berhasil *log-on* upaya sejak sukses *log-on* terakhir;
		• Tidak menampilkan *password* yang dimasukkan
		• Tidak mengirimkan *password* dalam bentuk teks melalui jaringan
		• Mengakhiri sesi aktif setelah periode tertentu tidak aktif, terutama di lokasi berisiko tinggi seperti area publik
		• Membatasi koneksi untuk memberikan keamanan tambahan untuk aplikasi berisiko tinggi
			akses aplikasi, apa saja data yang baru dimasukkan, di ubah, maupun dihapus	pelanggaran yang mulai terdeteksi
				• Menampilkan proses *log-on* antara lain:
				  ○ Tanggal dan waktu sukses *log-on*
				  ○ *Log-on* berhasil hingga *log-on* terakhir
				• Tidak menampilkan *password* yang diinputkan
				• Tidak bisa mencopas *password* dalam bentuk teks
				• Membatasi sesi *log-on* dalam periode tertentu jika sistem aplikasi sudah tidak digunakan
				• Membatasi koneksi internet untuk memberikan keamanan tambahan pada aplikasi maupun komputer yang digunakan

A.9.4.3 Sistem Manajemen *password*	Sistem manajemen *password* harus interaktif dan harus	• Menerapkan penggunaan user ID dan *password*	• Data instansi hanya bisa dimasukkan, diganti atau dihapus oleh *database*	• Adanya prosedur yang telah berjalan untuk

	memastikan kualitas *password*	untuk menjaga akuntabilitas • Memungkinkan pengguna untuk memilih dan mengubah *password* mereka sendiri dan menerapkan prosedur konfirmasi untuk kesalahan input; • Menegakkan pilihan *password* berkualitas • Memaksa pengguna untuk mengubah *password* mereka pada pertama *log-on* • Menegakkan perubahan *password* secara teratur dan sesuai kebutuhan • Mempertahankan catatan *password* yang digunakan sebelumnya dan mencegah pengguna Kembali • Tidak menampilkan *password* pada layer Ketika sedang masuk • Menyimpan dan mengirimkan *password* dalam bentuk enkripsi	teknisi saja. Sehingga para staff tidak dapat memodifikasi data yang sifatnya rahasia • Adanya prosedur yang telah berjalan untuk melakukan pergantian password ○ Setiap 3 bulan sekali sistem secara otomatis meminta teknisi untuk melakukan perubahan *password*	melakukan pergantian *password* ○ Setiap 3 bulan sekali sistem secara otomatis meminta teknisi untuk melakukan perubahan *password* • Memungkinkan pengguna untuk memilih dan mengubah *password* mereka sendiri dan menerapkan prosedur konfirmasi untuk kesalahan input; • Mewajibkan staf menggunakan *password* yang berkualitas ○ Panjang minimal 8 karakter ○ Wajib menggunakan huruf kapital, angka dan simbol • Tidak menampilkan *password* di layar Ketika sedang masuk • Menyimpan dan mengirim *password* dalam bentuk enkripsi • Mencegah penggunaan *password* yang sama dengan sebelumnya saat pergantian *password*

A.11.2.3	Listrik dan kabel telekomunikasi yang membawa data atau mendukung layanan informasi harus dilindungi dari gangguan atau kerusakan	• Listrik dan telekomunikasi sebaiknya ditanam dibawah tanah dan diberi perlindungan alternatif yang memadai • Kabel listrik harus dipisahkan dari kabel komunikasi untuk mencegah gangguan • Untuk sistem sensitif atau kritis, kontrol yang dipertimbangkan seperti: o Instalasi saluran lapis baja dan mengunci kotak pada inspeksi o Menggunakan perisai elektromagnetik untuk melindungi kabel o Pemeriksaan fisik untuk perangkat yang tidak sah yang melekat pada kabel o Mengontrol akses ke *patch panel* dan kabel room	• Adanya pengaturan kabel dengan melakukan pelabelan untuk masing-masing fungsi kabel o Adanya label di setiap ujung kabel o Adanya pembedaan warna kabel • Instansi memastikan peletakan kabel yang teratur dan tidak berantakan	• Membuat perlindungan teratur yang memadai seperti penanaman kabel bawah tanah • Pemisahan kabel telekomunikasi dengan kabel listrik untuk menghindari terjadinya korsleting • Pembuatan pelindung kabel agar tidak ada hewan pengerat maupun akses dari orang yang tidak berwenang • Melakukan pemeriksaan fisik secara berkala untuk menghindari perangkat tidak sah yang terhubung • Mengontrol akses pada panel patch dan kabel pada ruangan secara rutin
A.11.2.4 Kontrol pemeliharaan peralatan	Perlengkapan harus dipelihara dengan benar untuk memastikan integritas dan ketersediaan secara terus menerus	• *Equipment* harus dipelihara dengan spesifikasi dan internal servis yang direkomendasikan pemasok;	• Instansi melakukan *maintenance* rutin setiap sebulan sekali pada perangkat TI o Setiap staff dapat melaporkan setiap	• Pemeliharaan *equipment*, harus sesuai dengan spesifikasi dan interval servis yang telah di rekomendasikan

		• Hanya personil yang berwenang yang boleh melakukan pemeliharaan dan perbaikan • Catatan harus disimpan dari semua actual kesalahan, dan semua pemeliharaan preventif dan korektif • Kontrol yang tepat harus dilaksanakan bila maintenance equipment telah dijadwalkan. Dengan mempertimbangkan apakah *maintenance* ini dilakukan oleh pihak eksternal, bila perlu maka informasi rahasia harus dibersihkan terlebih dahulu dari *equipment, equipment* Kembali ke dalam operasi setelah *maintenance*, harus dipastikan bahwa peralatan tersebut berfungsi dan tidak rusak	terjadinya kerusakan pada perangkat TI yang digunakan pada bagian operasional ○ Bagian operasional mencatat setiap kejadian kerusakan dan melaporkan pada teknisi instansi maupun eksternal ○ Teknisi instansi maupun teknisi eksternal diwajibkan mencatat setiap komponen yang di ganti maupun setiap merubah konfigurasi pada perangkat TI • Adanya penguncian pada ruang server sehingga tidak dapat sembarang orang bisa masuk • Instansi melakukan maintenance WIFI setiap 2 minggu sekali • Adanya anggota satuan keamanan yang berkeliling Selama 24 jam penuh • Adanya camera CCTV yang memantau perlengkapan	• Adanya hak akses khusus untuk melakukan pemeliharaan dan perbaikan pada *equipment* instansi • Membuat form catatan pada semua kendala dan pemeliharaan *perfective* maupun korektif • Adanya penyimpanan catatan pelaporan kerusakan dan pemeliharaan secara preventif maupun korektif • Adanya penjadwalan yang tepat atau sesuai dengan rekomendasi dari pihak pemasok *equipment* • Membuat kontrol yang sesuai dengan kebutuhan untuk merekomendasikan sebelum melakukan *maintenance* dengan pihak eksternal

			• Instansi melakukan pengecekan kerusakan ruangan setiap 1 bulan sekali	
12.3.1 *Backup* Informasi	Backup cadangan dari informasi penting, *software* dan system image harus diambil dan diuji secara berkala sesuai dengan kebijakan yang disepakati	• Dokumentasi yang akurat dan lengkap dari Salinan *backup* dan prosedur dokumentasi harus dibuat • Frekuensi backup harus mencerminkan kebutuhan bisnis organisasi • *Backup* harus disimpan dilokasi terpencil, pada jarak yang cukup untuk menghindari bencana pada lokasi utama • Informasi *backup* harus diberi tingkat perlindungan fisik dan lingkungan yang konsisten • Media *backup* harus diuji secara teratur untuk memastikan bahwa mereka dapat diandalkan • *Backup* harus dilindungi dengan cara enkripsi	• Instansi melakukan *backup* data camera CCTV selama 1 bulan 2 kali • Adanya dokumentasi data dalam bentuk laporan cetak pada setiap sistem, yang dimiliki ○ Penyimpanan laporan cetak dilakukan denga cara terstruktur • Instansi melakukan *backup* server 2 hari sekali	• Membuat prosedur atau aturan *backup* yang lengkap dan sesuai kebutuhan ○ Dilakukan dokumentasi setiap melakukan backup ○ Frekuensi melakukan *backup* harus sesuai dengan kepentingan dan kebutuhan sebuah data bagi instansi ○ *Backup* data harus disimpan pada tempat yang aman dari terjadinya bencana ○ Lokasi *backup* harus diberi keamanan fisik dan lingkungan yang aman ○ Melakukan pengujian lokasi *backup* secara berkala ○ *Backup* data harus dilindungi dengan enkripsi

12.4.1 Pencatatan kegiatan	*Event log* merekam aktivitas pengguna, *exceptions*, kesalahan dan kejadian keamanan informasi harus diproduksi, disimpan secara berkala	• Merekam aktivitas berikut: • User ID • System activities • Tanggal, waktu dan rincian peristiwa penting, misalnya *log-on dan log-off* • Identitas perangkat atau lokasi jika mungkin dan sistem pengenal • Dokumentasi upaya *success* dan *reject access system* • Perubahan konfigurasi sistem • Penggunaan hak akses *privileged* • Pengguna sistem utilitas dan aplikasi • File diakses dan jenis akses • Alamat jaringan dan *protocol* • Meningkatkan alarm pada kontrol akses • Aktivasi dan de-aktivasi sistem perlindungan, seperti sistem anti-virus • Dokumentasi transaksi yang dilakukan oleh pengguna pada aplikasi	• Instansi memiliki catatan *log* setiap aktivitas dalam sistem informasi yang dimiliki *misalkan log login* siapa saja yang akses aplikasi, apa saja data yang baru dimasukkan, di ubah maupun dihapus • Adanya dokumentasi data dalam bentuk laporan cetak pada setiap sistem yang dimiliki ○ Penyimpanan laporan cetak dilakukan dengan terstruktur	○ Dokumentasi upaya *success dan reject* akses sistem perlindungan seperti sistem anti-virus ○ Dokumentasi transaksi yang dilakukan oleh pengguna pada aplikasi

12.4.2 Perlindungan informasi *log*	Fasilitas *logging dan log* informasi harus dilindungi terhadap gangguan dan akses yang tidak sah	• Memiliki dokumentasi terhadap perubahan jenis pesan • Melindungi file *log* yang sedang diedit atau dihapus • Menghindari kapasitas penyimpanan media file *log* yang sudah berlebih, sehingga gagal untuk melakukan penyimpanan	• Instansi memiliki catatan log setiap aktivitas dalam sistem informasi yang dimiliki misalkan log login siapa saja yang akses aplikasi, apa saja data yang baru dimasukkan di ubah, maupun dihapus • Adanya dokumentasi data dalam bentuk laporan cetak pada setiap sistem yang dimiliki • Data instansi hanya bisa dimasukkan, diganti atau dihapus oleh database teknisi saja. Sehingga para staff tidak dapat memodifikasi data yang sifatnya rahasia	• Adanya perlindungan khusus pada file log yang diedit maupun dihapus • Adanya pengecekan secara berkala pada kapasitas database untuk penyimpanan media file logging yang sudah berlebih, untuk mengurangi terjadinya kegagalan dalam pencatatan log atau kegiatan dalam setiap aktivitas yang dilakukan
12.4.3 *Log* Teknisi dan operator	Kegiatan *login system* teknisi dan sistem operator harus dilindungi secara berkala	• Melindungi dan meninjau log untuk menjaga akuntabilitas pengguna akses *privileged*	• Adanya autentikasi untuk *login* pengguna • instansi telah membedakan *role* atau hak akses untuk masing-masing pegawai sesuai dengan unit kerja dan fungsinya • setiap system memilik *user* level direktur, kepala bagian, dan staff memiliki *user interface system* yang berbeda	• adanya perbedaan hak akses untu teknisi khusus dalam melakukan perlindungan dan meninjau data *log* untuk menjaga akuntabilitas dan penggunaan akses *privileged*

			○ setiap sistem memiliki *user* level, direktur, kepala bagian, dan staff memiliki user *interface system* yang berbeda	

LAMPIRAN 11

HASIL PERENCANAAN KEBIJAKAN

KB - 01. KEBIJAKAN PENGENDALIAN HAK AKSES

AngkasaPura | AIRPORTS	*INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT*		
	KB 01	NO. RILIS	: 00
		NO. REVISI	: 00
	KEBIJAKAN PENGENDALIAN HAK AKSES	TANGGAL TERBIT	:
		HALAMAN	:

1. TUJUAN

Kebijakan berikut ini dibuat untuk menjamin persyaratan pengendalian hak akses terhadap informasi dan fasilitas informasi yang dimiliki agar dapat di definisikan dengan cepat

2. RUANG LINGKUP

Kebijakan ini berlaku untuk pihak-pihak yang terkait dengan penggunaan dalam menggunakan sistem informasi, sistem informasi yang dimaksud dalam kebijakan tersebut meliputi:

- *Flight Information Display System* (FIDS)
- Aplikasi Counter *check-in*

3. REFERENSI

3.1 ISO/IEC 27002:2013 – 9.1.1 Kebijakan pengendalian kontrol akses

3.2 ISO/IEC 27002:2013 – 12.4.1 Pencatatan kejadian

4. KEBIJAKAN

4.1 Pengelolaan hak akses sistem informasi

a) Hak akses pada setiap sistem informasi yang terkait dengan informasi instansi harus dibedakan sesuai peran dan fungsi dari masing – masing

pengguna.

b) Pemberian hak akses pada sistem informasi penggunaannya harus dibatasi berdasarkan tugas pokok dan fungsi pengguna dan harus disetujui oleh kepala divisi pada unit bisnis terkait dan kepala bagian personalia selaku penanggung jawab

c) Pemberian hak akses sistem informasi yang tingkatnya tinggi (*root*, super *user*, atau teknis) hanya diberikan kepada pegawai yang benar-benar kompeten, memiliki pengalaman kerja kurang lebih 3 tahun dan mendapat rekomendasi dari kepala divisi unit bisnis terkait dengan sistem informasi

d) Setiap pemberian hak akses sistem aplikasi pada pengguna harus disertai dengan kontrak tanggung jawab terkait tanggung jawab yang diberikan.

e) Setiap proses pengelolaan baik penghapusan maupun pemberian hak akses harus di dokumentasikan

f) Hak akses yang sudah diberikan tidak boleh digunakan maupun di pinjamkan kepada orang lain tanpa adanya ijin dan pemberitahuan perubahan hak akses baru

g) Dilakukan peninjauan secara langsung pengguna yang diberikan hak akses minimal 2 kali dalam sebulan

h) Dokumentasi wajib disertai dengan user ID, aktivitas yang dilakukan tanggal dan waktu, waktu peristiwa, hak akses yang di berikan, tanda tangan pengguna sistem, tanda tangan kepala bagian ICT.

4.2. Pengelolaan hak akses – pihak ketiga

4.2.1 Vendor, konsultan, mitra, atau pihak ketiga lainnya yang melakukan akses pada sistem aplikasi PT Angkasa Pura harus menandatangani ketentuan/Persyaratan Menjaga Kerahasiaan Informasi

4.2.2 Pemberian hak akses pihak ketiga dapat dilakukan setelah ada konfirmasi dari PT Angkasa Pura 1 Surabaya dan pihak ketiga

4.2.3 Setiap hak akses yang diberikan pada pihak ketiga harus ditinjau dan dibatasi waktunya

4.2.4 Setiap kegiatan yang dilakukan pihak ketiga harus didokumentasikan

4.2.5 Dokumentasi wajib disertai dengan *User ID*, Aktivitas yang dilakukan, tang gal dan waktu peristiwa, hak akses yang diberikan, tanda tangan pihak ketiga yang diberi akses, tanda tangan kepala bagian ICT.

5. DOKUMEN TERKAIT

PO 01 Prosedur Pengelolaan Hak Akses

IK - 02. KEBIJAKAN KEAMANAN INFORMASI

AngkasaPura | AIRPORTS	*INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT*		
	IK 02	NO. RILIS	: 00
		NO. REVISI	: 00
	KEBIJAKAN KEAMANAN INFORMASI	TANGGAL TERBIT	:
		HALAMAN	:

1. TUJUAN

Kebijakan berikut ini dibuat untuk menjamin keamanan dari informasi penting baik informasi digital dan fisik yang dimiliki instansi.

2. RUANG LINGKUP

Kebijakan ini berlaku untuk pihak-pihak yang terkait dengan penggunaan dalam menggunakan sistem aplikasi dan menjaga keamanan informasi yang berupa data elektronik. Data elektronik yang dimaksud dalam kebijakan tersebut meliputi:

- Basis Data
- Aplikasi
- Sistem Operasi
- File

3. REFERENSI

3.1. ISO/IEC 27002:2013 – 5.1.1 Kebijakan untuk keamanan informasi

3.2. ISO/IEC 27002:2013 – 6.1.1 Peran dan tanggung jawab

3.3. ISO/IEC 27002:2013 – 9.4.1 Pembatasan Akses Informasi

3.4. ISO/IEC 27002:2013 – 9.4.2 Prosedur *log-on* yang aman

3.5. ISO/IEC 27002:2013 – 9.4.3 Sistem Manajemen *Password*

3.6. ISO/IEC 27002:2013 – 12.3.1 *Backup* Informasi

3.7. ISO/IEC 27002:2013 – 12.4.1 Pencatatan Kejadian

3.8. ISO/IEC 27002:2013 – 12.4.2 Perlindungan Informasi *log*

3.9. ISO/IEC 27002:2013 – 12.4.3 *Log administrasi* dan operator

4. KEBIJAKAN

4.1 Pengelolaan sistem informasi (aplikasi)

4.1.1 Pada setiap sistem aplikasi yang dimiliki asset instansi wajib diberi perbedaan hak akses disesuaikan dengan fungsi dan unit bisnis yang dilakukan

4.1.2 Pada setiap sistem aplikasi yang dimiliki instansi diharuskan ada menu admin untuk melakukan kontrol pada pengguna pada sistem aplikasi tertentu

4.1.3 Pada setiap sistem operasi dan sistem aplikasi wajib diberikan log-on sistem untuk memverifikasi hak akses pengguna yang menggunakan sistem.

4.1.4 Pada setiap sistem aplikasi output yang di hasilkan dari sistem harus dibatasi sesuai dengan hak akses yang dimiliki

4.1.5 Pada setiap sistem aplikasi wajib adanya log-on event atau pencatatan kegiatan

4.1.6 Menghindari terjadinya kapasitas penyimpanan media file *log* yang sudah berlebih, dengan melakukan backup teratur

4.1.7 *Log-event* yang ada pada setiap sistem wajib di dokumentasikan atau di cetak setiap 2 minggu sekali untuk melakukan peninjauan dari kegiatan pengguna pada sistem tersebut

4.1.8 Dokumentasi log pada sistem wajib disertai dengan:

a. User ID,
b. Aktivitas pada sistem
c. Tanggal dan waktu,
d. Waktu peristiwa
e. Jenis hak akses
f. File yang diakses,
g. Nyala dan tidaknya kontrol pengamanan pada sistem (seperti antivirus, *firewall*)
h. Transaksi yang dilakukan pada sistem

4.2. Pengelolaan sistem *Log-on*

4.2.1 Tidak menampilkan pengidentifikasian sistem atau tampilan aplikasi sampai proses *log-on* dan selesai.

4.2.2 Menampilkan peringatan pemberitahuan umum bahwa computer hanya bisa diakses oleh pengguna yang berwenang.

4.2.3 Tidak menyediakan pesan bantuan selama procedure secure *log-on* berlangsung yang bisa memberikan bantuan kepada pengguna yang tidak berwenang

4.2.4 Validasi informasi *log-on* hanya jika seluruh data yang dibutuhkan diisi secara lengkap dan benar. Jika sebuah kondisi eror muncul, sistem tidak boleh menunjukkan bagian data mana yang benar dan yang salah.

4.2.5 Batasi jumlah kesempatan *log-on* gagal yang diizinkan

4.2.6 Wajib mencatat berapa kali gagal *log-on* untuk menghindari akses tidak berwenang.

4.2.7 Adanya pesan pengingat untuk maksimal percobaan *login*.

4.2.8 Karakter *password* disembunyikan.

4.3. Pengelolaan *password* pengguna

4.3.1 menerapkan *user* ID dan *password* pada setiap sistem untuk menjaga akuntabilitas.

4.3.2 Pengguna dapat merubah *password* mereka sendiri tetapi dengan syarat dan ketentuan yang ada.

4.3.3 *Password* yang digunakan wajib menggunakan *password* yang berkualitas

4.3.4 Perubahan *password* dilakukan dengan teratur selama 3 minggu sekali.

4.3.5 Tidak menggunakan *password* yang sama saat pergantian *password*.

4.3.6 Tidak menampilkan *password* saat *login* pada sistem.

4.3.7 *Password* yang dikirim ke *database* dikirim dalam bentuk enkripsi.

4.4. Pengelolaan *backup* dan *restore* informasi

4.4.1 *backup* hanya dapat dilakukan oleh *administrator*.

4.4.2 Adanya dokumentasi lengkap dari backup maupun *restore* data yang dilakukan.

4.4.3 Frekuensi *backup* dilakukan secara teratur dan sesuai kebutuhan bisnis dari organisasi.

4.4.4 Data atau informasi hasil backup dan dokumentasi disimpan dalam tempat yang aman untuk menghindari terjadinya bencana pada lokasi sebelumnya.

4.4.5 Informasi *backup* harus diberi tingkat perlindungan fisik dan lingkungan yang konsisten

4.4.6 Media untuk melakukan *backup* wajib diuji secara teratur

4.4.7 Data *backup* wajib dilindungi dengan enkripsi

4.5. Keamanan dan pengendalian informasi

4.5.1 pengendalian informasi internal dan *public* hanya diberikan kepada pegawai yang memiliki hak akses tertentu

4.5.2 keamanan informasi ini diberikan dan dipertanggung jawabkan setiap individunya dengan identifikasi pengguna informasi masing-masing.

4.5.3 Keamanan informasi ini juga dapat disahkan dengan bagian tertinggi menandatangani sebelum disebar luaskan.

4.5.4 Informasi diberikan otorisasi guna mencegah terjadinya penyalahgunaan dalam informasi tersebut.

4.5.5 Informasi ini berhubungan dengan data yang menjadi sumber dari informasi, penanggung jawab dan akses untuk informasi itu sendiri.

5. DOKUMEN TERKAIT

5.1 PO 02 Prosedur pengelolaan *password*

5.2 PO 03 Prosedur *Backup* dan *restore*

5.3 PO 07 Keamanan Informasi

IK - 03. KEBIJAKAN PENGELOLAAN *HARDWARE* DAN JARINGAN

AngkasaPura | AIRPORTS	*INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT* Seksi Pemeliharaan Infrastruktur TI		
	KB 02	NO. RILIS	: 00
		NO. REVISI	: 00
	KEBIJAKAN KEAMANAN INFORMASI	TANGGAL TERBIT	:
		HALAMAN	:

1. TUJUAN

Kebijakan berikut ini dibuat untuk menjamin fasilitas perangkat hardware dan jaringan agar dapat selalu beroperasi selama proses bisnis berlangsung.

2. RUANG LINGKUP

Kebijakan ini berlaku untuk pihak-pihak yang terkait dalam pengelolaan baik pemeliharaan maupun pengamanan *hardware* dan jaringan yang ada pada PT Angkasa Pura 1 Surabaya. *Hardware* dan jaringan yang dimaksud dalam kebijakan tersebut meliputi:

- *Server*
- Perangkat PC
- Printer
- Kamera CCTV
- *Router*
- Switch
- *Fire Alarm*
- *Access door*
- *X-Ray, WMTD, Body Scanner*
- Kabel Listrik
- Kabel Jaringan

3. REFERENSI

3.1. ISO/IEC 27002:2013 – 11.2.3 Pengendalian Keamanan Kabel

3.2. ISO/IEC 27002:2013 – 11.2.4 Kontrol Pemeliharaan Peralatan

4. KEBIJAKAN

4.1 Pengelolaan *Hardware*

4.1.1 Setiap ruangan diberikan pendingin ruangan untuk menghindari overheat (panas berlebih) pada perangkat *hardware*.

4.1.2 Server berada pada ruangan khusus yang dapat diakses oleh teknisi aja.

4.1.3 Setiap ruangan dilengkapi CCTV untuk menghindari pencurian.

4.1.4 Setiap ruangan dilengkapi *fire alarm* untuk mengidentifikasi jika terjadi kebakaran dan *fire extinguisher* (alat pemadam) untuk menghindari kemungkinan risiko kebakaran yang meluas.

4.1.5 Setiap kerusakan kendala perangkat *hardware* IT pada setiap unit, wajib segera dilaporkan kepada kepala divisi dan melaporkan kepada pihak divisi personalia selaku penanggung jawab.

4.1.6 Dilarang melakukan maintenance atau mengotak atik perangkat *hardware* tanpa adanya izin dari pihak staff seksi persandian dan keamanan informasi.

4.1.7 Dilarang menambahkan perangkat lain ke perangkat *hardware* yang ada pada instansi.

4.1.8 Dilarang mengambil atau membawa pulang perangkat *hardware* yang dimiliki instansi tanpa izin dari kepala staff seksi persandian dan keamanan informasi.

4.1.9 Setiap 3 bulan sekali wajib dilakukan maintenance perangkat *hardware* oleh pihak ketiga yang sudah menjalin Kerjasama dan persetujuan dari bidang seksi pemeliharaan infrastruktur TI.

4.1.10 *Maintenance* yang dilakukan harus mengikuti ketentuan dan peraturan instansi PT Angkasa Pura 1 Surabaya.

4.1.11 Divisi personalia wajib memastikan perangkat *hardware* yang di *maintenance* dapat digunakan Kembali dalam kegiatan operasional instansi.

4.1.12 Setiap kerusakan, kendala, peminjaman, *maintenance* wajib di dokumentasikan.

4.2. Pengelolaan jaringan

4.2.1 Dibuatkan perlindungan alternatif untuk seluruh kabel yang ada pada PT Angkasa Pura 1 Surabaya.

4.2.2 Dilakukan pelabelan sesuai fungsinya di setiap kabel pada PT Angkasa Pura 1 Surabaya.

4.2.3 Dilakukan pembedaan warna kabel untuk mempermudah proses *maintenance* dan pemasangan kabel.

4.2.4 Kabel telekomunikasi dan kabel listrik di tempatkan pada tempat berbeda

untuk menghindari terjadinya korsleting.

4.2.5 Setiap kerusakan, kendala perangkat jaringan pada setiap unit bisnis, wajib segera dilaporkan kepada kepala divisi dan melaporkan kepada pihak divisi personalia selaku penanggung jawab.

4.2.6 Setiap 3 bulan sekali wajib dilakukan maintenance perangkat jaringan seperti wifi, oleh pihak ketiga yang sudah menjalin Kerjasama dan persetujuan dari kepala bagian ICT.

4.2.7 Setiap kerusakan, kendala, *maintenance hardware* wajib di dokumentasikan.

5. DOKUMEN TERKAIT

5.1 PO 04 Prosedur Pengelolaan *Hardware*

5.2 PO 05 Prosedur Pengelolaan kabel dan jaringan telekomunikasi

IK - 04. KEBIJAKAN *HUMAN RESOURCE SECURITY*

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT Sekretariat		
	KB 02	NO. RILIS	: 00
		NO. REVISI	: 00
	KEBIJAKAN *HUMAN RESOURCE SECURITY*	TANGGAL TERBIT	:
		HALAMAN	:

1. TUJUAN

Kebijakan ini dibuat untuk memberikan peraturan kepada seluruh civitas instansi dalam memberi perlindungan keamanan pada aset yang dimiliki instansi.

2. RUANG LINGKUP

Kebijakan ini berlaku untuk pengguna yang menggunakan seluruh fasilitas asset informasi yang ada pada PT Angkasa Pura 1 Surabaya. Pengguna dimaksud tersebut antara lain:

- Pegawai PT Angkasa Pura 1 Surabaya
- Pegawai Magang
- Pihak Ketiga

3. REFERENSI

3.1. ISO/IEC 27002:2013 – 7.1.2 Syarat dan ketentuan kerja

3.2. ISO/IEC 27002:2013 – 7.2.2 Kepedulian Pendidikan dan pelatihan keamanan informasi

3.3. ISO/IEC 27002:2013 – 9.3.1 Penggunaan informasi autentikasi rahasia.

4. KEBIJAKAN

4.1 Keamanan Sumber Daya Manusia

4.1.1 Setiap pegawai pada instansi harus menandatangani dan menyetujui perjanjian (*non-disclosure*) hak akses sebelum diberikan akses pada asset pengelolaan informasi

4.1.2 Setiap pihak ketiga yang melakukan akses harus menandatangani dan menyetujui perjanjian (*non-disclosure*) hak akses sebelum diberikan

akses pada asset pengelolaan.

4.1.3 Setiap pegawai pada instansi harus diberikan pelatihan tentang kesadaran keamanan informasi yang dilakukan setiap 3 bulan sekali.

4.1.4 Pegawai magang pada instansi harus diberikan pelatihan dan pemahaman sebelum menggunakan hak akses dan memulai magang.

4.1.5 Kepala bagian personalia berhak untuk melakukan rotasi atau pergantian pegawai yang dinilai tidak relevan pada hak akses yang di berikan dengan persetujuan kepala bidang masing-masing.

4.1.6 Setiap pegawai dilakukan evaluasi kinerja secara berkala pada tiap akhir bulan oleh kepala bidang masing-masing.

4.1.7 Setiap pegawai yang hak aksesnya diganti ataupun dihentikan wajib mengisi form pengelolaan akses Kembali yang di setujui kepala bidang masing-masing.

4.2. Tanggung jawab penggunaan hak akses

4.2.1 Menghormati dan melindungi privasi orang lain, pengguna teknisi harus menghormati privasi orang lain Ketika mengetahui informasi yang bersifat pribadi dan harus mengambil Tindakan pencegahan yang tepat untuk melindungi informasi tersebut dari penggunaan oleh orang yang tidak berwenang.

4.2.2 Menyimpan autentikasi informasi rahasia, memastikan bahwa tidak dibocorkan kepada pihak lain. Pengguna yang memiliki hak akses wajib menjaga informasi rahasia instansi baik informasi dalam aplikasi maupun informasi dalam bentuk fisik atau cetakan dan memastikan informasi disimpan pada tempat yang aman untuk menghindari akses dari pihak yang tidak berwenang.

4.2.3 PC dan perangkat pengelolaan informasi terlindungi. Teknisi maupun pengguna memastikan tidak adanya perangkat lain yang terhubung ke sistem informasi pengelolaan instansi, memastikan *antivirus* dan *firewall* menyala saat digunakan dan pengguna tidak diperbolehkan menginstall aplikasi lain selain yang sudah disediakan instansi.

4.2.4 Memastikan pengguna *password* berkualitas, menggunakan *password* Panjang minimal 8 dan menggunakan semua karakter huruf, angka dan symbol.

4.2.5 Melindungi *password* yang digunakan dalam mengakses sistem pengelolaan informasi harus dilindungi. Setiap pengguna maupun teknisi bertanggung jawab untuk melindungi *password* yang dimiliki dan tidak membagikannya dengan orang lain, pengguna tidak diperkenankan menggunakan *password* yang sama dengan akun hak akses lainnya.

5. DOKUMEN TERKAIT

5.1 PO 06 Prosedur Pelatihan dan Pengembangan SDM

LAMPIRAN 12

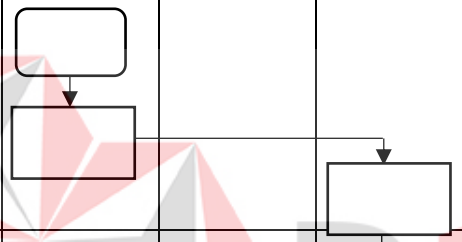
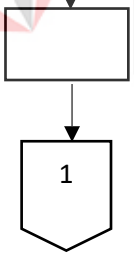
HASIL PERENCANAAN PROSEDUR

1. PROSEDUR PENGELOLAAN HAK AKSES

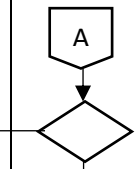
AngkasaPura | AIRPORTS	Nomor SOP	PO 01
	Tgl. Pembuatan	
	Tgl. Revisi	
	Tgl. Efektif	
	Disahkan Oleh	General Manager
	Nama SOP	PERENCANAAN HAK AKSES
DESKRIPSI SOP	KLASIFIKASI DAN DAFTAR PELAKSANAAN	
Prosedur pengelolaan hak akses merupakan prosedur untuk penggunaan hak akses terhadap sistem informasi dan penggunaan hak akses terhadap sistem informasi yang seharusnya dikontrol dalam rangka melindungi keamanan data baik dari dalam maupun dari luar instansi.	DAFTAR PELAKSANAAN 1. Pengguna sistem (staff pegawai) 2. Teknisi 3. Kepala ICT 4. Kepala persandian dan keamanan informasi	
KETERKAITAN		
	KUALIFIKASI PELAKSANA.	

1. KB 01 Kebijakan pengendalian hak akses 2. IK 01 Perubahan Hak Akses	- Memiliki kemampuan pemahaman proses bisnis yang baik - Memiliki pemahaman penggunaan sistem yang baik - Memiliki kemampuan komunikasi yang baik - Memiliki tanggung jawab kerja - Telah mengikuti pelatihan penggunaan sistem informasi
REFERENSI	PERLENGKAPAN/PERSYARATAN
ISO 27002:2013 – 9 Kontrol Akses 9.1 Persyaratan bisnis untuk akses kontrol 9.2 kebijakan pengelolaan kontrol akses 9.3 Manajemen akses pengguna 9.2.3 Pengelolaan Hak Akses Khusus	1. Media komunikasi: *Email* 2. FM 01 Formulir Pengelolaan Hak akses 3. FM 02 Formulir kontrak perjanjian hak akses 4. FM 03 Formulir *log* pengelolaan hak akses
PERINGATAN	PENCATATAN DAN PENDATAAN
Jika SOP ini tidak dijalankan maka pemberian akses kepada sistem pengelolaan informasi tidak sesuai dengan standar keamanan sehingga dapat mengakibatkan kerugian yang ada pada instansi (contoh kehilangan data, manipulasi data, akses oleh pihak yang tidak berwenang)	Teknisi sistem mencatat perubahan hak akses

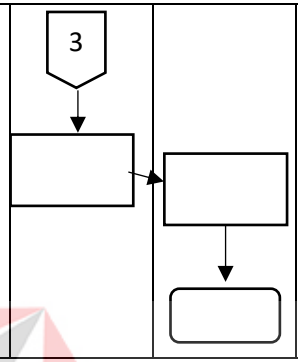
BAGAN ALUR - PO.1 Pengelolaan Hak akses

No.	SUB – AKTIVITAS	PELAKSANA				MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	4	Kelengkapan	Waktu	*Output*	
1.	Proses Pemberian akses sistem pengelolaan informasi instansi								
1.1	Mengajukan permintaan hak akses baru pada teknisi (via, *email*, maupun langsung)					- komputer - Koneksi internet - Media komunikasi (telephone, *email*)	1 hari	Surat pengajuan permintaan	
1.2	Menanyakan beberapa informasi kepada kepala seksi persandian dan keamanan informasi, mengenai Data					- komputer - Koneksi internet - Informasi data pegawai	1 hari	Data yang dibutuhkan	

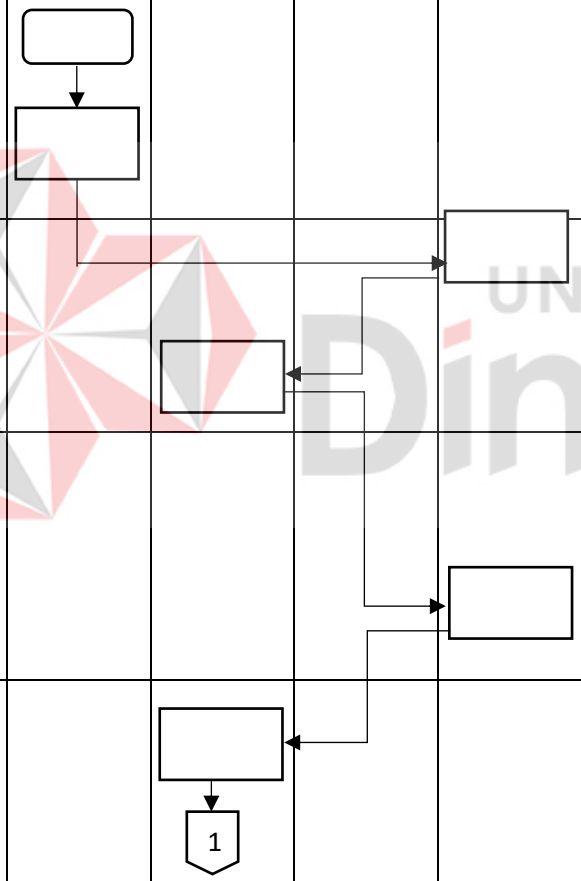
No.	SUB – AKTIVITAS	PELAKSANA				MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	4	Kelengkapan	Waktu	*Output*	
1.	Proses Pemberian akses sistem pengelolaan informasi instansi								
	pegawai yang diberikan akses, sistem informasi yang di akses, alasan pemberian hak akses		1						
1.3	Memberikan balasan terkait informasi yang diminta pada kepala seksi persandian dan keamanan					- Komputer - Koneksi internet - Media komunikasi (*telephone, email*)	2 hari	Surat balasan permintaan pemberian hak akses	
1.4	Melakukan pengirisan formulir pada formulir pengelolaan hak akses					- ATK	1 hari	Formulir pengelolaan hak akses	FM 01 Formulir Pengelolaan Hak Akses
			A						

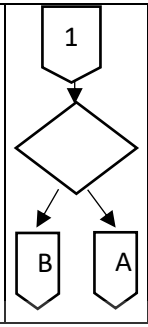
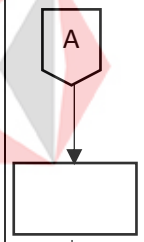
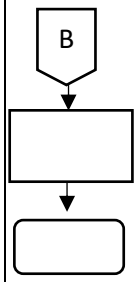
No.	SUB – AKTIVITAS	PELAKSANA				MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	4	Kelengkapan	Waktu	*Output*	
1.5	Melakukan persetujuan dengan kepala ICT					- ATK - Komputer - Koneksi Internet	2 hari	Surat persetujuan permintaan pemberian hak akses	FM 01 Formulir Pengelolaan Hak Akses
A.1	Disetujui: Jika pegawai telah mengikuti peraturan, hak akses sesuai dengan jabatan, mampu mengoperasikan sistem dengan baik					- Komputer - Koneksi internet - Media komunikasi (telephone, *email*)	2 hari	Surat balasan permintaan pemberian hak akses	
B.1	Tidak disetujui: Teknisi memberikan informasi terkait persetujuan ditolak karena pengguna tidak					- Komputer - Koneksi internet - Media komunikasi (telephone, *email*)	1 hari	Formulir pengelolaan hak akses	FM 01 Formulir Pengelolaan Hak Akses

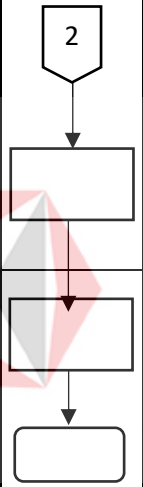
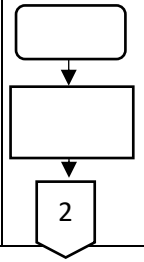
No.	SUB – AKTIVITAS	PELAKSANA				MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	4	Kelengkapan	Waktu	*Output*	
	Memenuhi kualifikasi dan proses selesai								
1.6	Memproses pemberian hak akses mengikuti instruksi perubahan hak akses		2			- Komputer - Koneksi internet - Media komunikasi (telephone, *email*)	1 hari	Informasi perubahan hak akses	
1.7	Memberikan informasi terkait status hak akses yang diberikan pada pegawai baru (via *email*, maupun secara langsung)					- Komputer - Koneksi internet - Media komunikasi (*telephone*, *email*)	2 hari	Informasi perubahan hak akses	IK 01 perubahan Hak Akses
1.8	Menerima informasi dari teknisi					- Koneksi internet	1 hari	Informasi pengelolaan hak akses	FM 01 Formulir Pengelolaan Hak Akses
1.9	Melakukan tanda tangan persetujuan hak akses	3				- ATK	1 Hari	Hasil kontrak persetujuan hak akses	FM 02 Formulir Kontrak Hak Akses
No.	SUB – AKTIVITAS	PELAKSANA				MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	4	Kelengkapan	Waktu	Output	

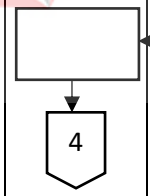
1.10	Memberikan ID, *password*, dan mencatat pada formulir *log* hak akses					- Koneksi internet - Media komunikasi (*telephone*, *email*)	1hari	ID dan *password* Hak Akses	FM 03 Formulir *log* pengelolaan hak akses

No.	SUB – AKTIVITAS	PELAKSANA				MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	4	Kelengkapan	Waktu	*Output*	
2.	Proses Penghapusan Hak Akses Informasi								
2.1	Mengajukan permintaan penghapusan akses baru pada teknisi (via, *email*, maupun langsung)					- Komputer - Koneksi internet - Media komunikasi (telephone, *email*)	1 Hari	Informasi penghapusan hak akses	
2.2	Menanyakan beberapa informasi mengenai data pegawai dan alasan penghapusan hak akses					- Koneksi internet - Media komunikasi (telephone, *email*)	1 hari	Informasi data pegawai	
2.3	Memberikan balasan terkait informasi yang diminta pada teknisi					- Komputer - Koneksi internet - Media komunikasi (*telephone*, *email*)	2 Hari	Informasi balasan penghapusan hak akses	
2.4	Melakukan pengisian formulir pada formulir pengelolaan hak akses					- ATK	1 hari	Formulir pengelolaan hak akses	FM 01 formulir pengelolaan hak akses



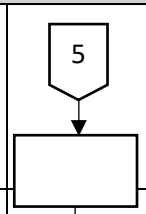
2.5	Melakukan persetujuan dengan kepala bagian aplikasi informatika					- Komputer - Koneksi internet - Media komunikasi (telephone, *email*)	2 hari	Informasi persetujuan	FM 01 formulir pengelolaan hak akses
No.	SUB – AKTIVITAS	PELAKSANA				MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	4	Kelengkapan	Waktu	*Output*	
A.1	Disetujui: Jika pegawai telah mengikuti peraturan, hak akses sesuai dengan jabatan mampu mengoperasikan sistem dengan baik					- Komputer - Koneksi internet - Media komunikasi (*telephone*, *email*)	2 Hari	Informasi balasan penghapusan hak akses	
2.4	Tidak disetujui: Teknisi memberikan informasi terkait persetujuan ditolak karena pengguna tidak memenuhi kualifikasi dan proses selesai					- ATK	1 hari	Formulir pengelolaan hak akses	FM 01 formulir pengelolaan hak akses

No.	SUB – AKTIVITAS	PELAKSANA				MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	4	Kelengkapan	Waktu	*Output*	
2.	Proses Penghapusan Hak Akses Informasi								
2.6	Memproses penghapusan hak akses mengikuti instruksi perubahan hak akses					- Komputer - Koneksi internet	1 Hari	Penghapusan hak akses	IK 01 Perubahan hak akses
2.7	Memberikan informasi terkait status hak akses yang diberikan pada calon pengguna (via,*email*,maupun secara langsung)					- Komputer - Koneksi internet - Media komunikasi (*telephone, email*, maupun secara langsung)	1 hari	Informasi status hak akses	IK 01 Perubahan Hak akses
3.	Proses Perubahan Hak Akses								
3.1	Mengajukan permintaan perubahan hak akses baru pada teknisi (via, email, telephone maupun secara langsung)					- Komputer - Koneksi internet - Media komunikasi (*telephone, email*, maupun	1 hari	Informasi pengajuan perubahan hak akses	

						secara langsung)			
3.2	Menanyakan beberapa informasi mengenai data pegawai dan alasan perubahan hak akses					- Komputer - Koneksi internet - Informasi data pegawai	2 hari	Informasi perubahan hak akses	
3.3	Memberikan balasan terkait informasi yang diminta pada teknisi					- Komputer - Koneksi internet - Media komunikasi (*email*)	1 hari	Informasi balasan	
3.4	Melakukan pengisian formulir pada formulir pengelolaan hak akses					- ATK	1 hari	Formulir pengelolaan gak akses	FM 01 formulir pengelolaan hak akses

3.	Proses Perubahan Hak Akses								
3.5	Melakukan persetujuan dengan kepala bagian aplikasi informatika	TIDAK	4			- Komputer - Koneksi internet - Media komunikasi (*email)*	1 Hari	Informasi persetujuan	FM 01 formulir pengelolaan hak akses
A1	Disetujui: Jika pegawai telah mengikuti pelatihan, hak akses sesuai dengan jabatan, mampu mengoperasikan sistem dengan baik		YA			- ATK	2 hari	Persetujuan di proses	
B1	Tidak disetujui: Teknisi memberikan informasi terkait persetujuan ditolak karena pengguna		4			- Komputer - Koneksi internet - Media komunikasi (*email*)	2 hari	Informasi penolakan	

3.	Proses Perubahan Hak Akses								
	Tidak memenuhi kualifikasi dan proses selesai		4						
A1	Disetujui: Jika pegawai telah mengikuti pelatihan, hak akses sesuai dengan jabatan, mampu mengoperasikan sistem dengan baik					- Komputer - Koneksi internet -	1 hari	Penghapusan hak akses	IK 01 Instruksi kerja perubahan hak akses
B1	Tidak disetujui: Teknisi memberikan informasi terkait persetujuan ditolak karena pengguna		5			- Komputer - Koneksi internet - Media komunikasi (*email*)	1 hari	Informasi status hak akses	

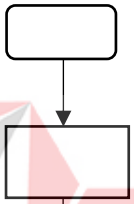
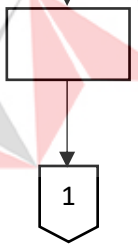
3.	Proses Perubahan Hak Akses								
3.8	Menerima informasi dari teknisi					- Komputer - Koneksi internet - Media komunikasi (*email*)	1 hari	Informasi hak akses	
3.9	Melakukan tanda tangan persetujuan hak akses					- ATK	1 hari	Persetujuan hak akses	FM 02 Formulir kontrak hak akses
3.10	Memberikan ID, *password* dan mencatatnya pada formulir *log* hak akses					- Koneksi internet - Media komunikasi (*email*)	1 hari	ID dan *password* hak akses	FM 03 formulir *log pengelolaan* hak akses

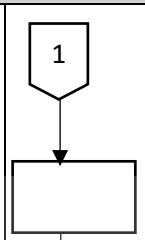
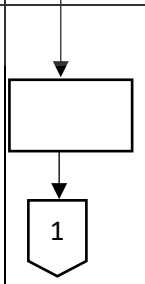
PO 02 PROSEDUR PENGELOLAAN *PASSWORD*

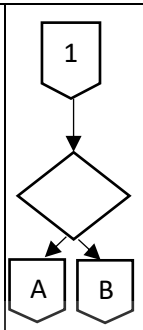
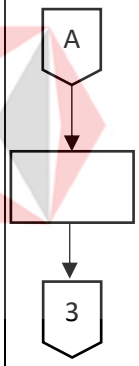
<table>
<tr><td rowspan="6">  </td><td>Nomor SOP</td><td>PO 02</td></tr>
<tr><td>Tgl. Pembuatan</td><td></td></tr>
<tr><td>Tgl. Revisi</td><td></td></tr>
<tr><td>Tgl. Efektif</td><td></td></tr>
<tr><td>Disahkan Oleh</td><td>General Manager</td></tr>
<tr><td>Nama SOP</td><td>PENGELOLAAN PASSWORD</td></tr>
<tr><td>DESKRIPSI SOP</td><td rowspan="3">KLASIFIKASI DAN DAFTAR PELAKSANAAN
DAFTAR PELAKSANAAN
1. General Manager
2. Teknisi
3. ICT
4. Pengguna sistem (staff/pegawai)
KUALIFIKASI PELAKSANA.
- Memiliki pemahaman Teknik dari kemampuan mengenai pemrograman
- Memiliki kemampuan dan pemahaman proses bisnis dengan baik
- Memiliki kemampuan berkomunikasi dengan baik</td></tr>
<tr><td>Prosedur manajemen password merupakan prosedur untuk memastikan pengelolaan pengguna password telah memenuhi kualitas standar password kuat dan memastikan password setiap pengguna sesuai dengan syarat kualitas password
KETERKAITAN
3. KB – 02 kebijakan keamanan informasi
4. IK – 02 instruksi kerja perubahan password
5. IK – 03 instruksi kerja reset password</td></tr>
<tr><td>REFERENSI
ISO 27001:2013 – 9 Kontrol Akses
9.4 Sistem dan Kontrol Akses Aplikasi
9.4.2 Prosedur log-on yang aman
9.4.3 Prosedur Manajemen password</td><td>PERLENGKAPAN/PERSYARATAN
- Media komunikasi: Email
- FM 04 Formulir Perbaikan sistem informasi
- FM 05 Formulir Permintaan reset password</td></tr>
</table>

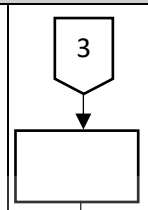
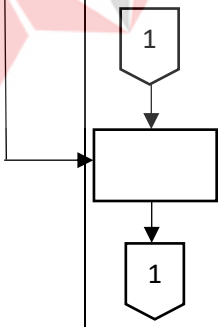
PERINGATAN	PENCATATAN DAN PENDATAAN
Jika SOP ini tidak dijalankan maka pengelolaan *password* pada sistem informasi tidak sesuai dengan standar keamanan informasi sehingga dapat mengakibatkan kerugian atau risiko yang ada pada instansi meliputi kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) data	- Pencatatan formulir perbaikan sistem informasi - Pencatatan formulir *reset password*

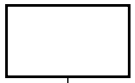
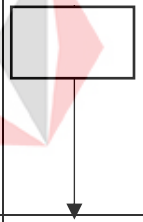
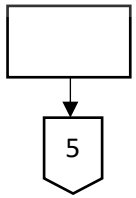
BAGAN ALUR – PO.2 Pengelolaan *Password*

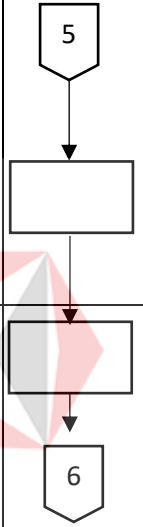
No.	SUB – AKTIVITAS	PELAKSANA				MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	4	Kelengkapan	Waktu	*Output*	
1.	Proses Perubahan *Password* kuat								
1.1	Menentukan standar pengguna *password* sesuai dengan kualitas standar *password* kuat					- Komputer - Koneksi internet - Media komunikasi *email*)	1 Hari	Informasi standar pengguna *password*	KB 03 Kebijakan Keamanan Informasi
1.2	Meminta admin untuk melakukan penambahan fitur *password* kuat dalam semua sistem informasi instansi					- Komputer - Koneksi internet - Media komunikasi *email*)	1 hari	Informasi penambahan fitur *password*	

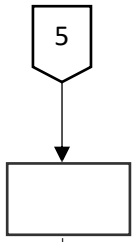
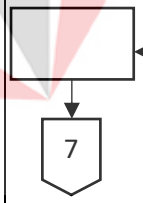
No.	SUB – AKTIVITAS	PELAKSANA				MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	4	Kelengkapan	Waktu	*Output*	
1.	Proses Perubahan *Password* kuat								
1.3	Melakukan Analisa kebutuhan sistem informasi untuk penambahan *password* kuat dan menentukan waktu pengerjaan					- Komputer - Koneksi internet	1 Hari	Informasi Analisa kebutuhan sistem	
1.4	Menambah fitur *password* kuat sesuai dengan waktu yang ditentukan					- Komputer - Koneksi internet	1 hari	Informasi penambahan *password*	
1.5	Memastikan seluruh sistem informasi yang membutuhkan prosedur *log-in* telah memiliki ketentuan inputan *password* kuat					- Komputer - Koneksi internet	1 hari	Informasi prosedur *log-in*	

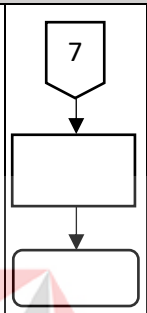
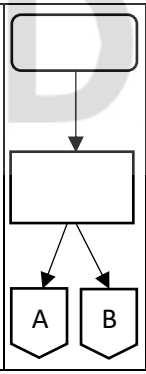
1.6	Melakukan pengujian terhadap fitur baru *password* kuat					- ATK - Komputer - Koneksi internet	2 hari	Informasi pengujian fitur baru	
1.7	Uji coba berhasil melakukan pelaporan kepada kepala pengembangan aplikasi					- ATK - Komputer - Koneksi internet	1 hari	Laporan uji coba status berhasil	

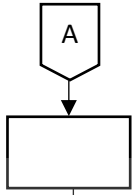
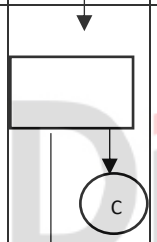
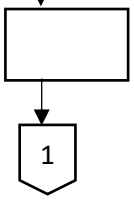
No.	SUB – AKTIVITAS	PELAKSANA				MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	4	Kelengkapan	Waktu	*Output*	
1.	Proses Perubahan *Password* kuat								
A2	Melakukan validasi dan persetujuan hasil penambahan fitur					- Komputer - Koneksi internet	1 hari	Validasi pertujuan penambahan fitur	
A3	Mengisi laporan perbaikan fitur pada sistem informasi pada formulir perbaikan sistem informasi					- ATK - Komputer - Koneksi internet	1 hari	Laporan perbaikan sistem	FM 04 formulir perbaikan sistem informasi
B1	Uji coba gagal Melakukan Kembali sub- proses 1.3					- Komputer - Koneksi internet	1 hari	Laporan uji coba status gagal	

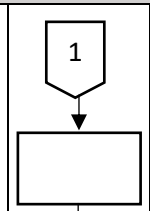
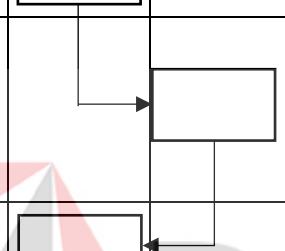
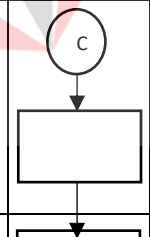
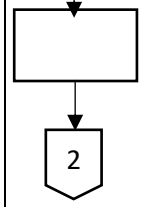
No.	SUB – AKTIVITAS	PELAKSANA				MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	4	Kelengkapan	Waktu	*Output*	
1.	Proses Perubahan *Password* kuat								
1.8	Mempersiapkan prosedur *password* lama dengan melakukan *setup* pada seluruh sistem					- ATK - Komputer - Koneksi internet	1 hari	Informasi prosedur perubahan	
1.9	Menyediakan *password* default sementara yang telah sesuai dengan standar kuat *password* untuk masing-masing pengguna sistem					- Komputer - Koneksi internet	1 hari	Informasi *password default* sementara	
1.10	Mensosialisasikan penambahan fitur baru kepada seluruh pegawai instansi					- Komputer - Koneksi internet	1 hari	Sosialisasi penambahan fitur	

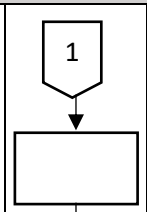
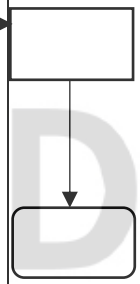
No.	SUB – AKTIVITAS	PELAKSANA				MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	4	Kelengkapan	Waktu	*Output*	
1.	Proses Perubahan *Password* kuat								
1.11	Mengirimkan *email* yang berisi *password default* sementara untuk seluruh pengguna sistem informasi mengenai ketentuan pengguna kualitas password					- Komputer - Koneksi internet - Media komunikasi (*email*)	1 hari	Informasi *password* default	
1.12	Melakukan *login* dengan menggunakan *password default* *t*					- Komputer - Koneksi internet - Media komunikasi (*email*)	1 hari	*Login* sementara	

No.	SUB – AKTIVITAS	PELAKSANA				MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	4	Kelengkapan	Waktu	*Output*	
1.	Proses Perubahan *Password* kuat								
1.13	Mengeluarkan notifikasi untuk meminta seluruh pegawai melakukan penggantian *password default* baru sesuai dengan ketentuan kualitas standar *password* kuat					- Komputer - Koneksi internet - Media komunikasi (*email*)	2 Hari	Notifikasi penggunaan *password* default	
1.14	Memastikan seluruh pegawai mengganti *password* default dalam kurun waktu kurang dari satu bulan					- Komputer - Koneksi internet - Media komunikasi (*email*)	1 bulan	Informasi mengganti *password* default	

No.	SUB – AKTIVITAS	PELAKSANA				MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	4	Kelengkapan	Waktu	*Output*	
1.	Proses Perubahan *Password* kuat								
1.14	Mengelola data penggunaan *password* lama dan memastikan tidak ada pengguna Kembali *password default*					- Data pengguna - Komputer - Koneksi internet - Media komunikasi (*email*)	2 Hari	Informasi pengelolaan data pengguna *password* lama	
2.	Proses Permintaan *Reset Password*								
2.1	Melakukan permintaan reset *password*: a. Secara langsung kepada Kepala ICT b. Via *email* kepada admin					- Komputer - Koneksi internet - Media komunikasi (*email*)	1 hari	Informasi permintaan *password*	

No.	SUB – AKTIVITAS	PELAKSANA				MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	4	Kelengkapan	Waktu	*Output*	
1.	Proses Perubahan *Password* kuat								
A1	Pengguna mengajukan permintaan *reset password* pada ICT					- Komputer - Koneksi internet - Media komunikasi (*email*)	2Hari	Informasi pengajuan *reset password*	
A2	Mengisi formulir permintaan reset *password* dan menyertakan permintaan *password*					- ATK	1hari	Formulir *reset password*	FM 05 formulir *reset password*
B1	Mengajukan permintaan reset *password* pada admin via *email*					- Komputer - Koneksi internet - Media komunikasi (*email*)	3hari	Informasi pengajuan reset *password*	

2.	Proses Permintaan *Reset Password*								
B2	Membalas dengan meminta data informasi terkait dengan pengguna sistem					- Komputer - Koneksi internet - Media komunikasi (*email*)	2 Hari	Notifikasi balasan	
B3	Mengirim informasi yang diminta					- Komputer - Koneksi internet - Media komunikasi (*email*)	1 hari	informasi pengguna sistem	
B4	Mengisi formulir *reset password*					- ATK	1 hari	Formulir reset *password*	FM 05 formulir *reset password*
2.2	Melakukan validasi pada permintaan reset *password*					- Komputer - Koneksi internet - Media komunikasi (*email*)	1 hari	Informasi validasi	
2.3	Melakukan reset *password* dengan mengikuti instruksi reset *password*					- Komputer - Koneksi internet - Media komunikasi (*email*)	1 hari	Informasi *reset password*	IK 04 Instruksi kerja *reset password*

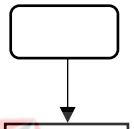
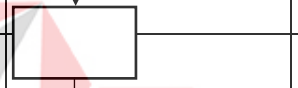
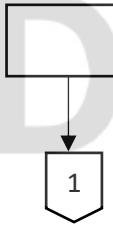
2.	Proses Permintaan *Reset Password*								
2.4	Mengirimkan email yang berisikan *password* sementara yang hanya dapat digunakan sementara					- Komputer - Koneksi internet - Media komunikasi (*email*)	2 Hari	Informasi *password* sementara	
2.5	Mengakses aplikasi dengan *password* baru lalu otomatis muncul notifikasi untuk segera mengganti *password*					- Komputer - Koneksi internet - Media komunikasi (*email*)	1 hari	Notifikasi ganti *password*	

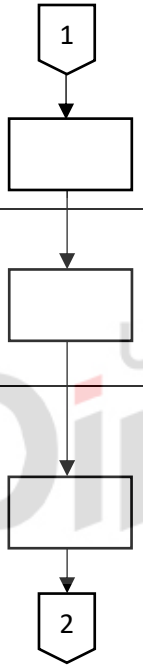
2. PROSEDUR *BACKUP* DAN *RESTORE*

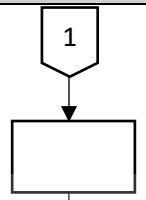
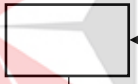
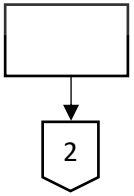
<table>
<tr><td rowspan="6">  </td><td>Nomor SOP</td><td>PO 03</td></tr>
<tr><td>Tgl. Pembuatan</td><td></td></tr>
<tr><td>Tgl. Revisi</td><td></td></tr>
<tr><td>Tgl. Efektif</td><td></td></tr>
<tr><td>Disahkan Oleh</td><td>General Manager</td></tr>
<tr><td>Nama SOP</td><td>BACKUP DAN RESTORE</td></tr>
<tr><td>DESKRIPSI SOP</td><td rowspan="3">KLASIFIKASI DAN DAFTAR PELAKSANAAN
DAFTAR PELAKSANAAN
5. General Manager
6. ICT
KUALIFIKASI PELAKSANA.
- Memiliki pemahaman Teknik dari kemampuan mengenai pemrograman
- Memiliki kemampuan dan pemahaman proses bisnis dengan baik
- Memiliki kemampuan berkomunikasi dengan baik</td></tr>
<tr><td>Prosedur backup dan restore data merupakan prosedur yang bertujuan untuk memastikan backup yang dilakukan secara berkala telah sesuai dan data yang di backup telah lengkap</td></tr>
<tr><td>KETERKAITAN
1. KB – 02 kebijakan keamanan informasi
2. IK – 04 Instruksi Backup data dan Restore
3. IK – 05 Instruksi Restore Data</td></tr>
<tr><td>REFERENSI</td><td>PERLENGKAPAN/PERSYARATAN</td></tr>
<tr><td>ISO 27002:2013 – 12 Keamanan operasi
12.3 Backup
12.3.1 Backup Informasi
12.4.3 log administrasi data operator</td><td>- Perangkat media backup dan restore
- FM 06 Formulir klasifikasi data
- FM 07 Formulir Log backup data
- FM 08 Formulir Restore Data</td></tr>
</table>

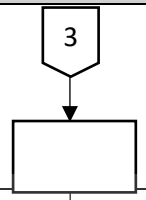
PERINGATAN	PENCATATAN DAN PENDATAAN
Jika SOP ini tidak dijalankan maka backup data tidak berjalan dengan baik sehingga dapat mengakibatkan risiko yang berkaitan dengan ketersediaan *(availability*) data serta terganggunya proses bisnis	- Pencatatan formulir perbaikan sistem informasi - Pencatatan formulir permintaan pergantian *password*

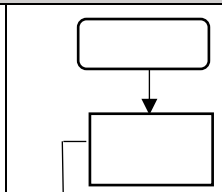
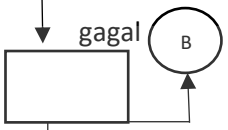
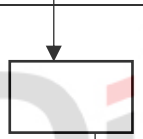
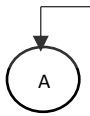
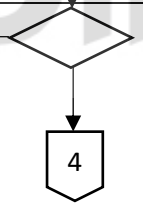
BAGAN ALUR – PO.03 *Backup* dan *Restore*

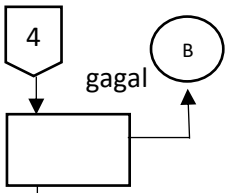
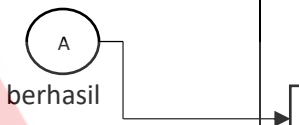
No.	SUB – AKTIVITAS	PELAKSANA		MUTU BAKU			Keterangan/Dok. Terkait
		1	2	Kelengkapan	Waktu	*Output*	
1.	Proses Umum sebelum melakukan Backup						
1.1	Melakukan klasifikasi data dan menentukan tingkat kritikalitas data			- Data *Backup* - Komputer - Koneksi internet	2 Hari	Informasi klasifikasi data	FM 06 formulir klasifikasi data
A1	Membuat strategi backup melakukan klasifikasi terhadap data dan menentukan tingkatan kritikalitas data untuk menentukan tipe *backup*			- Data *Backup* - Komputer - Koneksi internet	1 hari	Menentukan strategi *backup*	

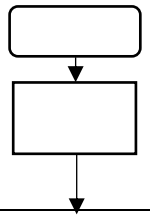
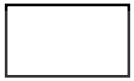
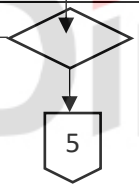
No.	SUB – AKTIVITAS	PELAKSANA		MUTU BAKU			Keterangan/Dok. Terkait
		1	2	Kelengkapan	Waktu	*Output*	
A2	Melakukan pembaharuan pada formulir data klasifikasi data			- ATK	1 hari	Pembaruan data pada formulir	FM 06 formulir klasifikasi data
A3	Membuat sebuah strategi untuk melakukan backup data sesuai dengan tipe *backup*			- Data Backup - Komputer - Koneksi internet -	1 hari	Membuat strategi *backup*	
A4	Menentukan jadwal untuk *backup* data dan tipe *backup*			- Data *Backup* - Komputer - Koneksi internet	2 hari	Jadwal backup	

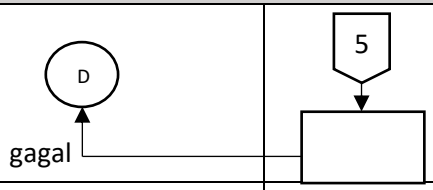
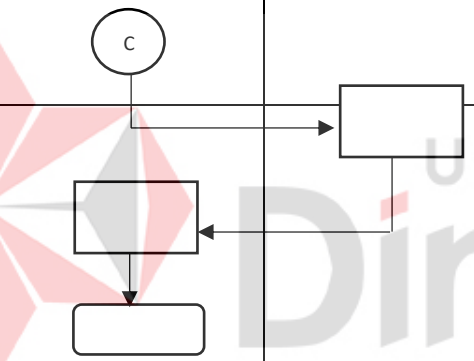
No.	SUB – AKTIVITAS	PELAKSANA		MUTU BAKU			Keterangan/Dok. Terkait
		1	2	Kelengkapan	Waktu	*Output*	
1.	Proses Umum sebelum melakukan Backup						
B1	Penentuan media backup ICT melakukan checklist pemeliharaan media *backup*			- Data *Backup* - Komputer - Koneksi internet	1 hari	Informasi penentuan media *backup*	
2.	Proses Backup data secara berkala						
2.1	Menginstruksikan untuk melakukan *backup* secara berkala			- Data *Backup* - Komputer - Koneksi internet	1 hari	Informasi *backup*	
2.2	Melakukan setting penjadwalan *backup* data			- Data *Backup* - Komputer - Koneksi internet	1 hari	Jadwal *backup*	

No.	SUB – AKTIVITAS	PELAKSANA		MUTU BAKU			Keterangan/Dok. Terkait
		1	2	Kelengkapan	Waktu	*Output*	
2.	Proses Backup Data secara Berkala						
2.3	Melakukan *monitoring* secara berkala untuk memastikan bahwa hasil edukasi *backup* data telah lengkap			- Data *Backup* - Komputer - Koneksi internet	1 hari	Hasil edukasi *backup* data lengkap	
2.4	Mengelola *log* pada sistem *backup*			- Data *Backup* - Komputer - Koneksi internet	2 hari	Pengelolaan *log* sistem *backup*	
2.5	Membuat laporan pada formulir *log backup* data			- Data *Backup* - Komputer - Koneksi internet	5 hari	Laporan *backup*	FM 07 Formulir *log backup* data
2.6	Memastikan bahwa ICT telah mengimplementasikan dan melakukan *monitoring* secara berkala			- Data *Backup* - Komputer - Koneksi internet	1 bulan	Informasi implementasi dan *monitoring* berkala	FM 07 Formulir *log backup* data

3.	Proses uji backup data secara berkala						
3.1	Melakukan uji *backup* data secara berkala 3 bulan sekali			- Data *Backup* - *Komputer* - Koneksi internet	3 bulan	Uji *Backup*	
3.2	Melakukan set *up* persiapan uji coba *backup* data			- Data *Backup* - Komputer - Koneksi internet	2 hari	Informasi set *up* uji *backup*	
3.3	Melakukan uji ciba backup data pada media *backup*			- Data *Backup* - Komputer - Koneksi internet	2 hari	Uji coba *backup* data	
3.4	Menganalisa *log backup* apakah *log backup* berhasil						

3.	Proses uji backup data secara berkala						
A1	Status gagal Melakukan Kembali proses uji ciba *backup* data pada sub-proses 3.2			- Data *Backup* - Komputer - Koneksi internet	6 hari	Informasi *backup* gagal	
B1	Status Berhasil Melakukan pengecekan kesesuaian data yang berhasil di *backup*			- Data *Backup* - Komputer - Koneksi internet	1 bulan	Informasi *backup* berhasil	
B2	Membuat laporan pada formulir uji coba *backup* data			- Data *Backup* - Komputer - Koneksi internet	6 hari	Laporan uji coba log *backup* data	FM 07 formulir log *backup* data

4.	Proses Restore Data						
4.1	Menentukan *database* yang dilakukan *restore*			- *Database* - Komputer - Koneksi internet	2 hari	Informasi *database restore*	
4.2	Menentukan jadwal pelaksanaan *restore* data			- *Database* - Komputer - Koneksi internet	2 hari	Jadwal *restore database*	
4.3	Melakukan proses *restore* data			- *Database* - K omputer - Koneksi internet	1 hari	*Restore database*	FM 08 Formulir *restore* data
4.4	Menganalisa hasil *restore* data apakah *restore* data berhasil?						

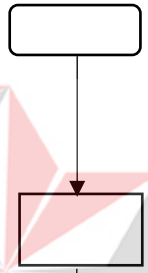
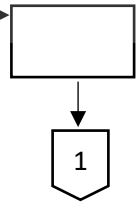
4.	Proses Restore Data						
A1	Gagal Seksi bagian pengembangan aplikasi melakukan kernbali sub-proses			- *Database* - Komputer - Koneksi internet	1 hari	Informasi *database restore* gagal	
B1	Berhasil Seksi bagian pengembangan aplikasi mendokumentasikan pelaksanaan *restore* data			- *Database* - Komputer - Koneksi internet	1 hari	Informasi *database restore* berhasil	FM 08 Formulir *restore* data
4.5	Memvalidasi formulir *restore* data			- *Database* - Komputer - Koneksi internet	2 hari	Informasi validasi *restore* data	

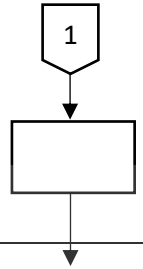
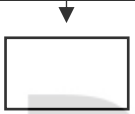
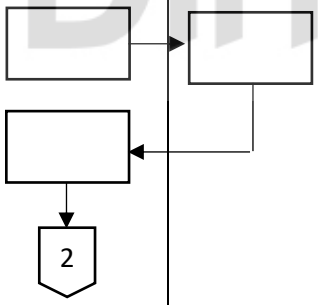
4. PROSEDUR PENGELOLAAN HARDWARE

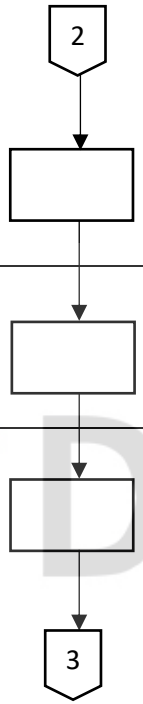
<table>
<tr><td rowspan="5">  </td><td>Nomor SOP</td><td>PO 04</td></tr>
<tr><td>Tgl. Pembuatan</td><td></td></tr>
<tr><td>Tgl. Revisi</td><td></td></tr>
<tr><td>Tgl. Efektif</td><td></td></tr>
<tr><td>Disahkan Oleh</td><td>General Manager</td></tr>
<tr><td>DESKRIPSI SOP</td><td>Nama SOP</td><td>PERAWATAN HARDWARE</td></tr>
<tr><td colspan="2">Prosedur Perawatan hardware ini merupakan pedoman dan acuan untuk melakukan pengelolaan aset hardware pada instansi baik dalam melaksanakan pengembangan, pengendalian dan pemeliharaan infrastruktur jaringan teknologi informasi dan komunikasi serta keamanan dari hardware itu sendiri.</td><td rowspan="3">KLASIFIKASI DAN DAFTAR PELAKSANAAN
DAFTAR PELAKSANAAN
- Seksi pemeliharaan infrastruktur teknologi informasi dan komunikasi
- Seksi pengendalian infrastruktur teknologi informasi dan komunikasi
KUALIFIKASI PELAKSANA.
- Memiliki pemahaman Teknis dan kemampuan mengenai hardware
- Memiliki kemampuan berkomunikasi dengan baik</td></tr>
<tr><td colspan="2">KETERKAITAN
1. KB – 03 Kebijakan pengelolaan hardware dan kabel jaringan telekomunikasi
2. IK – 06 infrastruktur kerja perawatan hardware</td></tr>
<tr><td colspan="2">REFERENSI
ISO 27002:2013 – 11 Keamanan Fisik dan Lingkungan
11.2 Peralatan
11.2.3 Pengendalian keamanan Kabel</td></tr>
<tr><td colspan="2">PERLENGKAPAN/PERSYARATAN
- Media komunikasi: email, telephone
- FM 04 Formulir perbaikan sistem informasi
- FM 09 formulir pemeliharaan perangkat TI</td></tr>
</table>

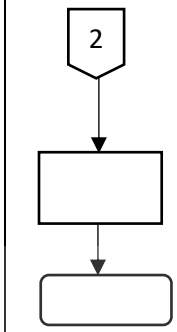
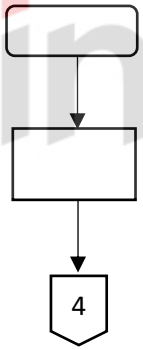
11.2.4 Kontrol Pemeliharaan Peralatan	- FM 10 formulir berita acara kerusakan - FM 11 formulir laporan evaluasi penggunaan perangkat TI -
PERINGATAN	PENCATATAN DAN PENDATAAN
Jika SOP ini tidak dijalankan maka pengelolaan asset *hardware* tidak sesuai dengan standar keamanan sehingga dapat mengakibatkan tergantungnya proses bisnis yang sedang berjalan di instansi.	- pegawai mencatat aktivitas pada formulir pemeliharaan perangkat TI - pegawai mencatat pada formulir berita acara setiap terjadinya kerusakan - pegawai mencatat semua pada formulir laporan evaluasi pengelolaan perangkat TI

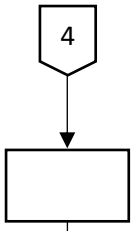
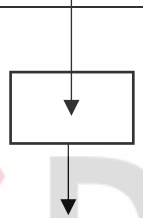
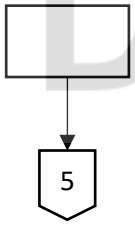
BAGAN ALUR – PO.04 Perawatan *Hardware*

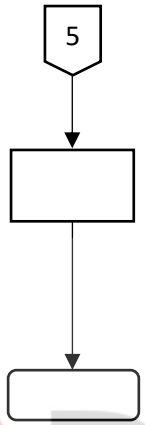
No.	SUB – AKTIVITAS	PELAKSANA			MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	Kelengkapan	Waktu	*Output*	
1.	Proses Pelaporan Kerusakan *Hardware*							
1.1	Melaporkan kerusakan *hardware* pada seksi pemeliharaan teknologi informasi dan komunikasi (via *email*, *telephone*, ataupun langsung)			-	- Komputer - Perangkat *hardware* - Media komunikasi (*email*, *telephone*, ataupun langsung)	4 hari	Laporan kerusakan *hardware*	KB 03 Kebijakan pengelolaan h*ardware* dan kabel jaringan komunikasi
1.2	Memproses laporan dengan membuat berita acara kerusakan terkait teknologi yang di laporkan			-	- Komputer - Media komunikasi	2 hari	Laporan berita acara	

No.	SUB – AKTIVITAS	PELAKSANA			MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	Kelengkapan	Waktu	*Output*	
1.	Proses Pelaporan Kerusakan *Hardware*							
1.3	Melakukan pengecekan pada *hardware* yang dilaporkan				- Komputer - Media komunikasi)	4 hari	Laporan pengecekan *hardware*	
1.4	Mencatat pada formulir laporan pengelolaan perangkat TI				- ATK - Komponen hardware - Media komunikasi	2 hari	Laporan pengelolaan perangkat TI	FM 11 formulir laporan pengelolaan perangkat TI
2.	Proses Pemeliharaan *hardware*							
2.1	Melakukan perbaikan *hardware* yang dilaporkan (perbaikan dilakukan sesuai dengan kebutuhan)				- Komponen *hardware* - Media komunikasi	2 hari	Perbaikan / penggantian komponen *hardware*	FM 09 formulir pemeliharaan perangkat TI

2.	Proses Pemeliharaan *hardware*							
2.2	Melakukan pencatatan kegiatan pemeliharaan hardware pada formulir pemeliharaan perangkat TI				- ATK - Komponen *hardware* - Media komunikasi	1 hari	Pencatatan pemeliharaan *hardware*	FM 09 formulir pemeliharaan perangkat TI
2.3	Memastikan hardware dapat digunakan kembali				- ATK - Komponen hardware - Media komunikasi	2 hari	Informasi *hardware* berjalan sesuai fungsi	
2.4	Melaporkan kepada kepala bidang aplikasi informatika untuk melakukan validasi berita acara kerusakan				- Komputer - Koneksi internet - Media komunikasi)	2 hari	Laporan validasi berita kerusakan *hardware*	FM 04 Formulir Perbaikan Sistem Informasi

2.	Proses Pemeliharaan *hardware*							
2.5	Mencatat pada formulir laporan pengelolaan perangkat TI				- Komputer - Koneksi internet - Media komunikasi)	2 hari	Laporan Pengelolaan perangkat TI	FM 09 formulir pemeliharaan perangkat TI
3.	Proses Perbaikan *Hardware* secara berkala							
3.1	Melakukan perawatan *hardware* dilakukan bersama dengan pihak vendor untuk pemeliharaan rutin *hardware* yang sudah ditentukan yaitu selama 6 bulan sekali				- ATK - Komponen *hardware* - Media komunikasi	6 bulan	Informasi perawatan rutin *hardware*	

3.	Proses Perbaikan *Hardware* secara berkala							
3.2	Melakukan pencatatan kegiatan pemeliharaan *hardware* pada formulir pemeliharaan perangkat TI				- ATK - Komponen *hardware* - Media komunikasi	1 bulan	Informasi pemeliharaan *hardware*	FM 09 formulir pemeliharaan perangkat TI
3.3	Memastikan *hardware* dapat digunakan				- ATK - Komponen *hardware* - Media komunikasi	3 hari	Informasi memastikan *hardware* berfungsi dengan baik	
3.4	Melaporkan kepada kepala bagian ICT untuk melakukan validasi formulir pemeliharaan TI				- ATK - Komponen *hardware* - Media komunikasi	6 bulan	Informasi perawatan rutin *hardware*	

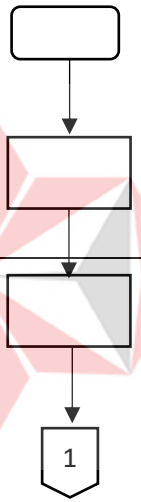
3.	Proses Perbaikan *Hardware* secara berkala							
3.5	Mencatat pada formulir laporan pengelolaan perangkat TI				- ATK - Komponen *hardware* - Media komunikasi	1 bulan	Informasi pencatatan pengelolaan *hardware*	FM 09 formulir pemeliharaan perangkat TI

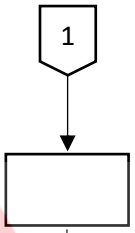
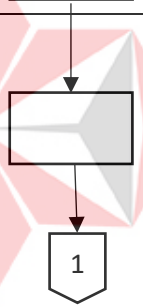
5. PROSEDUR PENGELOLAAN KABEL JARINGAN TELEKOMUNIKASI

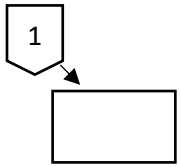
<table>
<tr><td rowspan="6">  </td><td>Nomor SOP</td><td>PO 05</td></tr>
<tr><td>Tgl. Pembuatan</td><td></td></tr>
<tr><td>Tgl. Revisi</td><td></td></tr>
<tr><td>Tgl. Efektif</td><td></td></tr>
<tr><td>Disahkan Oleh</td><td>General Manager</td></tr>
<tr><td>Nama SOP</td><td>KEAMANAN KABEL</td></tr>
<tr><td>DESKRIPSI SOP</td><td>KLASIFIKASI DAN DAFTAR PELAKSANAAN</td></tr>
<tr><td>Prosedur keamanan kabel merupakan prosedur yang berguna untuk memastikan bahwa seluruh kabel telekomunikasi yang membawa data dan mendukung layanan informasi pada instansi atau dikelola secara teratur sehingga terlindungi dari kerusakan</td><td rowspan="2">DAFTAR PELAKSANAAN
- Seksi jaringan infrastruktur teknologi informasi dan komunikasi
- Seksi pemeliharaan infrastruktur teknologi informasi dan komunikasi
- Bidang infrastruktur teknologi informasi dan komunikasi
KUALIFIKASI PELAKSANA.
- Memiliki pemahaman Teknis dan kemampuan mengenai hardware
- Memiliki kemampuan berkomunikasi dengan baik</td></tr>
<tr><td>KETERKAITAN
1. KB 03 Kebijakan pengelolaan hardware dan kabel jaringan telekomunikasi
2. IK 07 instruksi kerja perawatan kabel telekomunikasi
3.</td></tr>
<tr><td>REFERENSI</td><td>PERLENGKAPAN/PERSYARATAN</td></tr>
<tr><td>ISO 27002:2013 – 11 Keamanan Fisik dan Lingkungan
11.2 Peralatan
11.2.3 Pengendalian keamanan Kabel</td><td>- FM 09 formulir pemeliharaan perangkat TI
- FM 10 formulir berita acara kerusakan</td></tr>
</table>

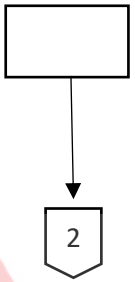
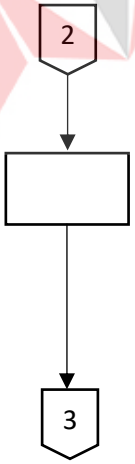
PERINGATAN	PENCATATAN DAN PENDATAAN
Jika SOP ini tidak dijalankan, maka dapat mengakibatkan terganggunya proses bisnis yang sedang berjalan di instansi	- Pencatatan pada formulir berita acara kerusakan - Pencatatan pada formulir pemeliharaan perangkat TI

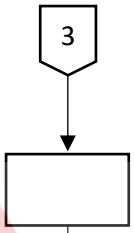
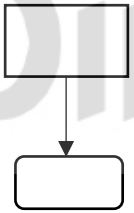
BAGAN ALUR – PO.05 Keamanan Kabel

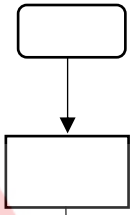
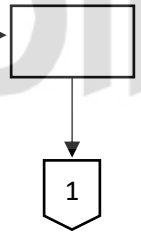
No.	SUB – AKTIVITAS	PELAKSANA		MUTU BAKU			Keterangan/Dok. Terkait
		1	2	Kelengkapan	Waktu	*Output*	
1.	Proses Pemeliharaan Kabel Telekomunikasi						
1.1	Seksi persandian dan keamanan membuat perlindungan alternative untuk seluruh kabel yang ada pada instansi			- Komponen kabel - Perangkat *hardware*	2 Hari	Informasi perlindungan alternative	
1.2	Seksi persandian dan keamanan melakukan pelabelan sesuai fungsinya di setiap kabel pada instansi			- Komponen kabel - Perangkat *hardware*	2 hari	Informasi pelabelan sesuai fungsi	

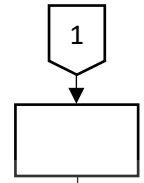
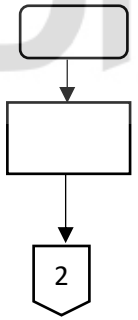
No.	SUB - AKTIVITAS	PELAKSANA		MUTU BAKU			Keterangan/Dok. Terkait
		1	2	Kelengkapan	Waktu	*Output*	
1.	Proses Pemeliharaan Kabel Telekomunikasi						
1.3	Seksi persandian dan keamanan melakukan pembedaan warna kabel untuk mempermudah proses *maintenance* dan pemasangan kabel			- Komponen kabel - Perangkat *hardware*	5 Hari	Informasi pembeda warna kabel dan pemasangan kabel	
1.4	Seksi persandian dan keamanan menempatkan kabel telekomunikasi dan kabel listrik di tempatkan pada tempat berbeda untuk menghindari terjadinya korsleting			- Komponen kabel - Perangkat *hardware*	5 hari	Informasi tempat letak kabel dan keamanan	

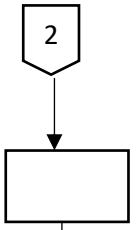
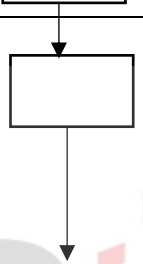
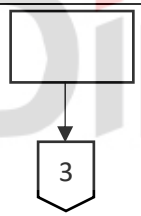
No.	SUB – AKTIVITAS	PELAKSANA		MUTU BAKU			Keterangan/Dok. Terkait
		1	2	Kelengkapan	Waktu	*Output*	
1.	Proses Pemeliharaan Kabel Telekomunikasi						
1.3	Seksi persandian dan keamanan melakukan pembedaan warna kabel untuk mempermudah proses			- Komponen kabel - Perangkat *hardware*	5 Hari	Informasi pembeda warna kabel dan pemasangan kabel	

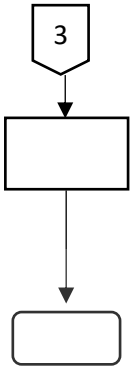
	maintenance dan pemasangan kabel						
1.4	Seksi persandian dan keamanan menempatkan kabel telekomunikasi dan kabel listrik di tempatkan pada tempat berbeda untuk menghindari terjadinya korsleting			- Komponen kabel - Perangkat hardware	5 hari	Informasi tempat letak kabel dan keamanan	
No.	SUB – AKTIVITAS	PELAKSANA		MUTU BAKU			Keterangan/Dok. Terkait
		1	2	Kelengkapan	Waktu	*Output*	
1.	Proses Pemeliharaan Kabel Telekomunikasi						
1.5	Seksi persandian dan keamanan membuat berita acara kerusakan terkait kendala perangkat jaringan pada setiap bidang			- ATK - Komponen kabel - Perangkat hardware	2 Hari	Informasi berita acara kerusakan setiap bidang	FM 10 Formulir berita acara kerusakan

No.	SUB – AKTIVITAS	PELAKSANA		MUTU BAKU			Keterangan/Dok. Terkait
		1	2	Kelengkapan	Waktu	*Output*	
1.	Proses Pemeliharaan Kabel Telekomunikasi						
1.6	Melakukan maintenance perangkat jaringan oleh pihak ketiga yang sudah menjalin kerja sama dengan instansi setiap 3 bulan sekali			- ATK - Komponen kabel - Perangkat *hardware*	3 bulan	Informasi pemeliharaan komponen kabel dan *hardware*	FM 09 Formulir Pemeliharaan Perangkat TI
1.7	Seksi persandian dan keamanan melaporkan hasil pemeliharaan kabel rutin kepada kepala ICT			- ATK - Komponen kabel - Perangkat *hardware*	5 hari	Informasi hasil pemeliharaan kabel secara rutin	FM 09 Formulir Pemeliharaan Perangkat TI

No.	SUB – AKTIVITAS	PELAKSANA		MUTU BAKU			Keterangan/Dok. Terkait
		1	2	Kelengkapan	Waktu	*Output*	
1.	Proses Pelaporan Kerusakan Kabel Jaringan Telekomunikasi						
1.1	Melaporkan kerusakan kabel jaringan telekomunikasi pada seksi pemeliharaan teknologi informasi dan komunikasi (via *email*, telepon maupun secara langsung)			- Komputer - Perangkat *hardware* - Media komunikasi - (*email, telepon*, maupun secara langsung)	1 hari	Laporan kerusakan kabel jaringan telekomunikasi	KB 03 Kebijakan pengelolaan *hardware* dan kabel jaringan komunikasi
1.2	Memproses laporan dengan membuat berita acara kerusakan terkait teknologi informasi yang dilaporkan			- Komputer - Media komunikasi	2 hari	Laporan berita acara	

No.	SUB – AKTIVITAS	PELAKSANA		MUTU BAKU			Keterangan/Dok. Terkait
		1	2	Kelengkapan	Waktu	*Output*	
1.	Proses Pelaporan Kerusakan Kabel Jaringan Telekomunikasi						
1.3	Melakukan pengecekan pada kabel jaringan telekomunikasi yang dilaporkan			- Komponen *hardware* - Perangkat *hardware*	2 hari	Laporan pengecekan kabel jaringan telekomunikasi	
1.4	Mencatat pada formulir laporan pengelolaan perangkat TI			- ATK - Komponen *hardware* - Perangkat *hardware*	2 hari	Laporan pengelolaan perangkat TI	FM 11 Formulir laporan pengelolaan perangkat TI
3.	Perbaikan Kabel Jaringan Telekomunikasi						
3.1	Melakukan perbaikan kabel jaringan telekomunikasi dilakukan Bersama dengan pihak vendor untuk melakukan pemeliharaan rutin *hardware* yang sudah ditentukan yaitu 6 bulan sekali			- ATK - Komponen *hardware* - Perangkat *hardware*	6 bulan	Informasi perbaikan rutin kabel jaringan telekomunikasi	
3.2	Melakukan pencatatan kegiatan perbaikan kabel jaringan			- ATK - Komponen *hardware*	1 bulan	Informasi pemeliharaan kabel jaringan telekomunikasi	FM 09 Formulir pemeliharaan perangkat TI

	telekomunikasi pada formulir pemeliharaan perangkat TI			- Media komunikasi			
3.3	Memastikan kabel jaringan telekomunikasi dapat digunakan kernbali			- ATK - Komponen *hardware* - Media komunikasi	3 hari	Informasi memastikan kabel jaringan telekomunikasi berfungsi dengan baik	
3.4	Melaporkan kepada kepala ICT untuk melakukan validasi formulir pemeliharaan TI			- ATK - Komponen *hardware* - Media komunikasi	6 bulan	Informasi perawatan rutin kabel jaringan telekomunikasi	

3.	Perbaikan Kabel Jaringan Telekomunikasi						
3.5	Mencatat pada formulir laporan pengelolaan perangkat TI			- ATK - Komponen *hardware* - Media komunikasi	1 bulan	Informasi pencatatan pengelolaan kabel jaringan telekomunikasi	FM 09 Formulir pemeliharaan perangkat TI

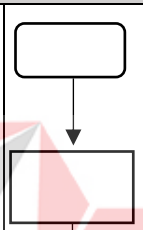
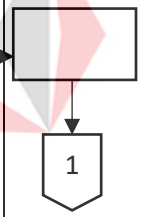
6. PROSEDUR PELATIHAN DAN PENGEMBANGAN SDM

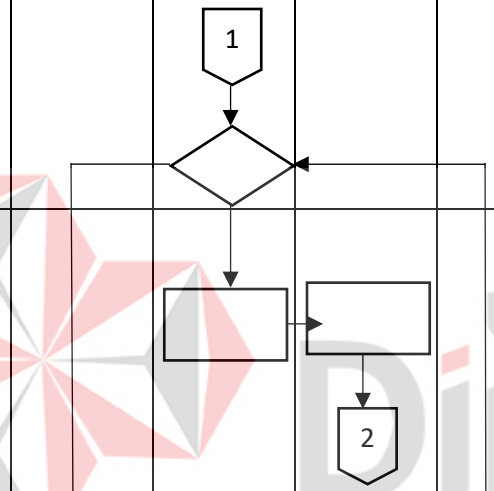
AngkasaPura | AIRPORTS	Nomor SOP	PO 06
	Tgl. Pembuatan	
	Tgl. Revisi	
	Tgl. Efektif	
	Disahkan Oleh	General Manager
	Nama SOP	PELATIHAN DAN PENGEMBANGAN SDM

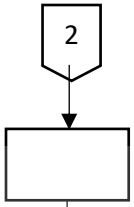
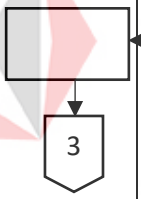
DESKRIPSI SOP	KLASIFIKASI DAN DAFTAR PELAKSANAAN
Prosedur Pelatihan dan Pengembangan SDM merupakan prosedur yang mengatur segala pelatihan atau edukasi terkait keamanan informasi untuk pegawai yang mampu meningkatkan kualitas baik secara intelektual maupun kepribadian. Sehingga mampu menjadi asset informasi yang dimiliki oleh instansi	DAFTAR PELAKSANAAN - Pegawai - Sekretariat - Staff bagian sekretariat - Kepala divisi ICT KUALIFIKASI PELAKSANA. - Memiliki akses penggunaan data instansi - Memiliki kemampuan pemahaman proses bisnis dengan baik - Memiliki kemampuan komunikasi dengan baik
KETERKAITAN	
1. KB 04 Kebijakan *Human Resource Security* 2. IK 08 instruksi kerja pelatihan dan pengembangan SDM instansi	
REFERENSI	PERLENGKAPAN/PERSYARATAN
ISO 27002:2013 – 7 Keamanan Sumber Daya Manusia 7.2 Keamanan selama bekerja 7.2.2 Kesadaran keamanan informasi, Pendidikan dan pelatihan	- Surat tugas - FM 12 Formulir data pegawai - FM 13 Formulir Evaluasi Kegiatan Pengembangan Kompetensi

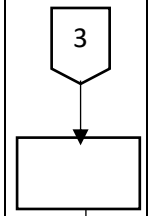
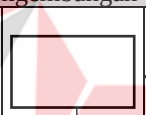
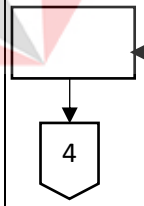
9 kontrol akses 9.3 tanggung jawab pengguna 9.3.1 Penggunaan informasi autentikasi rahasia	
PERINGATAN	PENCATATAN DAN PENDATAAN
Jika SOP ini tidak dijalankan, maka pegawai lebih mudah lalai dalam agenda mengelola informasi instansi sehingga dapat mengakibatkan risiko hilangnya data serta dapat merusak citra instansi	- Pencatatan formulir data pegawai - Pencatatan formulir evaluasi kegiatan pengembangan kompetensi

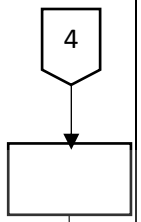
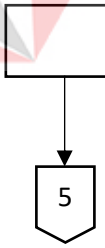
BAGAN ALUR – PO.06 Pelatihan dan Pengembangan SDM

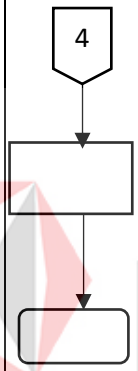
No.	SUB – AKTIVITAS	PELAKSANA				MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	4	Kelengkapan	Waktu	*Output*	
1.	Proses Pendaftaran Pelatihan dan Pengembangan								
1.1	Membuat permintaan pendaftaran kegiatan pengembangan kompetensi					- Komputer - Koneksi internet - Media komunikasi (*email*)	2 hari	Informasi permintaan kegiatan	
1.2	Membuat permohonan keikut sertaan dalam kegiatan tersebut					- Komputer - Koneksi internet - Media komunikasi (*email*)	1 hari	Pembuatan permohonan ikut serta kegiatan	

No.	SUB – AKTIVITAS	PELAKSANA				MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	4	Kelengkapan	Waktu	*Output*	
1.	Proses Pendaftaran Pelatihan dan Pengembangan								
	Apakah permohonan tersebut di setujui								
A1	Disetujui: Melanjutkan proses					- Komputer - Koneksi internet - Media komunikasi - Surat permohonan	2 hari	Informasi permohonan disetujui	
A2	Tidak di setujui: Melakukan kembali sub-proses 1.2					- Komputer - Koneksi internet - Media komunikasi - Surat permohonan	2 hari	Informasi permohonan ditolak	

No.	SUB – AKTIVITAS	PELAKSANA				MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	4	Kelengkapan	Waktu	*Output*	
1.	Proses Pendaftaran Pelatihan dan Pengembangan								
1.4	Memberikan informasi mengenai kegiatan pengembangan kompetensi yang diadakan					- Komputer - Koneksi internet - Media komunikasi	1 hari	Informasi kegiatan	
2.	Proses Persiapan Pelatihan dan Pengembangan								
2.1	Membuat persiapan dari kegiatan tersebut					- ATK - Koneksi internet - Media komunikasi	1 hari	Persiapan peserta	

2.	Proses Persiapan Pelatihan dan Pengembangan								
2.2	Pemberian surat tugas								
3.	Proses Pelatihan dan Pengembangan								
3.1	Hadir pelatihan					- ATK	1 hari	Daftar hadir peserta pelatihan	FM 12 Formulir Data Pegawai
3.2	Peserta melakukan presensi kehadiran					- ATK	1 hari	Daftar hadir peserta pelatihan	FM 12 Formulir Data Pegawai
3.3	Membuat catatan semua kegiatan pelatihan dalam formulir data pegawai					- ATK - Koneksi internet - Media komunikasi	1 hari	Catatan peserta dan catatan kegiatan	

No.	SUB – AKTIVITAS	PELAKSANA				MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	4	Kelengkapan	Waktu	*Output*	
4.	Proses Evaluasi Pelatihan								
4.1	Membuat laporan sebagai pertanggung jawaban ke pihak kepala bidang, paling lambat 1 bulan					- ATK - Koneksi internet - Media komunikasi	1 bulan	Pembuatan laporan pertanggung jawaban	
4.2	Laporan pertanggung jawaban kegiatan pelatihan dan pengembangan					- ATK - Koneksi internet - Media komunikasi	2 hari	Laporan pertanggung jawaban pelatihan	
4.3	Melakukan evaluasi menggunakan formulir evaluasi kegiatan pengembangan kompetensi					- ATK - Koneksi internet - Media komunikasi	3 hari	Evaluasi kegiatan pelatihan kompetensi	FM 13 Formulir evaluasi pelatihan

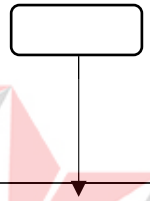
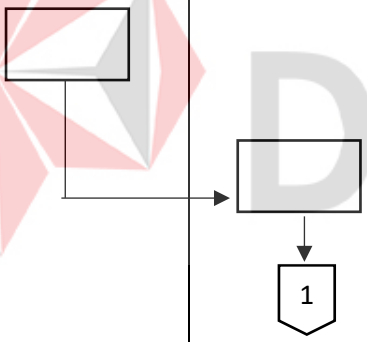
No.	SUB – `AKTIVITAS	PELAKSANA				MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	4	Kelengkapan	Waktu	*Output*	
4.	Proses Evaluasi Pelatihan								
4.5	Mempertimbangkan penilaian tahunan pegawai					- ATK - Koneksi internet - Media komunikasi	14 hari	Penilaian tahunan pegawai	

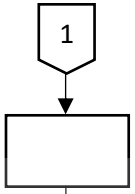
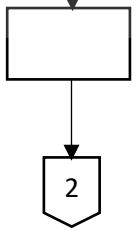
7. PROSEDUR KEAMANAN INFORMASI

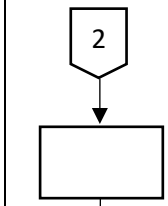
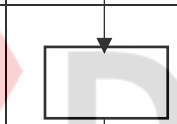
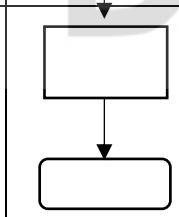
<table>
<tr><td rowspan="6">  </td><td>Nomor SOP</td><td>PO 07</td></tr>
<tr><td>Tgl. Pembuatan</td><td></td></tr>
<tr><td>Tgl. Revisi</td><td></td></tr>
<tr><td>Tgl. Efektif</td><td></td></tr>
<tr><td>Disahkan Oleh</td><td>General Manager</td></tr>
<tr><td>Nama SOP</td><td>KEMANAN INFORMASI</td></tr>
<tr><td colspan="2">DESKRIPSI SOP</td><td>KLASIFIKASI DAN DAFTAR PELAKSANAAN</td></tr>
<tr><td colspan="2">Prosedur keamanan informasi merupakan prosedur yang mengatur tentang keamanan asset informasi internal dan publik untuk meningkatkan kualitas informasi yang baik dari kualitas informasi yang diberikan kepada pembaca atau mencari pada instansi atau pun publik</td><td rowspan="3">DAFTAR PELAKSANAAN
- Sekretariat
- ICT
- Seksi Persandian dan Keamanan Informasi
KUALIFIKASI PELAKSANA.
- Memiliki akses penggunaan data informasi instansi
- Memiliki kemampuan pemahaman proses bisnis dengan baik
- Memiliki kemampuan komunikasi dengan baik</td></tr>
<tr><td colspan="2">KETERKAITAN</td></tr>
<tr><td colspan="2">1. KB 02 Kebijakan
2. IK 09 Instruksi Kerja
3. IK 10 Instruksi Kerja</td></tr>
<tr><td colspan="2">REFERENSI</td><td>PERLENGKAPAN/PERSYARATAN</td></tr>
<tr><td colspan="2">ISO 27002:2013 – 5 Kebijakan Keamanan Informasi
5.1 Arahan manajemen untuk keamanan informasi
5.1.1 Kebijakan untuk keamanan informasi</td><td>- FM 06 Formulir Klasifikasi data
- FM 14 Monitoring Keamanan Informasi</td></tr>
</table>

6 Organisasi Keamanan Informasi 6.1 Organisasi internal 6.1.1 Peran dan tanggung jawab	
PERINGATAN	PENCATATAN DAN PENDATAAN
Jika SOP ini tidak dijalankan, maka informasi disampaikan tidak akurat dan dapat mengakibatkan risiko kehilangan kepercayaan serta dapat merusak citra instansi	- Pencatatan klasifikasi data informasi pada formulir klasifikasi data - Pencatatan monitoring keamanan informasi yang disampaikan pada formulir monitoring keamanan informasi

BAGAN ALUR – PO.07 Keamanan Informasi

No.	SUB – AKTIVITAS	PELAKSANA			MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	Kelengkapan	Waktu	*Output*	
1.	Klasifikasi Keamanan Informasi							
1.1	Klasifikasi data untuk mendukung informasi di berikan kepada ICT dan untuk proses pengklasifikasian informasi				- Computer - Koneksi internet - Media komunikasi (*email*)	2 hari	Informasi klasifikasi data	FM 06 Formulir Klasifikasi Data
1.2	Klasifikasi data dibedakan untuk mempermudah penyampaian informasi				- Computer - Koneksi internet - Media komunikasi (*email*)	1 hari	Informasi klasifikasi data	FM 06 Formulir Klasifikasi Data

No.	SUB – AKTIVITAS	PELAKSANA			MUTU BAKU			Keterangan/Dok. Terkait
		1	2	3	Kelengkapan	Waktu	*Output*	
1.	Klasifikasi Keamanan Informasi							
1.3	Pembuatan informasi sesuai dengan kebutuhan informasi				- Computer - Koneksi internet - Media komunikasi (*email*)	2 hari	Informasi	FM 06 Formulir Klasifikasi Data
1.4	Informasi yang disebarkan harus memiliki otoritas informasi agar tidak dapat disalahgunakan oleh pihak yang tidak bertanggung jawab				- Computer - Koneksi internet - Media komunikasi (*email*)	2 hari	Informasi yang sip untuk di publish	
1.5	Melakukan monitoring dan evakuasi tentang informasi yang di publish apakah sudah sesuai atau belum?				- Computer - Koneksi internet - Media komunikasi (*email*)	2 hari	Monitoring informasi	FM 14 Formulir Monitoring Keamanan Informasi

2.	Peran dan tanggung jawab informasi							
2.1	ICT memberikan peran dan tanggung jawab untuk informasi yang disampaikan				- ATK - Koneksi internet - Media komunikasi	1 hari	Peran dan tanggung jawab	
2.2	Penandatanganan peran dan tanggung jawab				- ATK	1 hari	Daftar peran dan tanggung jawab	
2.3	Informasi siap di publish di bandara				- ATK	1 hari	Informasi	
2.4	Proses monitoring informasi setelah informasi disebar				- ATK - Koneksi internet - Media komunikasi	3 hari	Monitoring informasi	FM 14 Formulir Monitoring Keamanan Informasi

LAMPIRAN 13

HASIL PERENCANAAN INSTRUKSI KERJA

IK – 01. INSTRUKSI KERJA PENGELOLALAN HAK AKSES

AngkasaPura | AIRPORTS	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication* and *Technology Department Head*		
	IK 01	NO. RILIS	: 00
		NO. REVISI	: 00
	INSTRUKSI KERJA PEMBERIAN HAK AKSES	TANGGAL TERBIT	:
		HALAMAN	:

1. PELAKSANA

Information Communication and *Technology Department Head*

2. RINCIAN INSTRUKSI KERJA

1. Pegawai mengajukan permintaan pemberian hak akses baru melalui *email*
2. Kepala ICT menanyakan kepada kepala seksi persandian dan keamanan informasi mengenai data pegawai yang diberi akses
3. Teknisi memberi balasan terkait dengan informasi yang diminta oleh kepala seksi persandian
4. Teknisi mengisi formulir pada form pengelolaan hak akses
5. Teknisi melakukan persetujuan dengan kepala ICT
    a. Jika pegawai telah mengikuti peraturan mengenai permintaan hak akses sesuai dengan jabatan, maupun mengoperasikan sistem maka proses pemberian hak akses untuk pegawai baru disetujui dan
    b. Lanjut pada proses pemberian hak akses dan mengikuti instruksi perubahan hak akses
    c. Jika pegawai tidak mengikuti peraturan yang telah diberikan oleh teknisi mengenai pemberian hak akses maka penolakan ditolak dan teknisi mengirimkan informasi penolakan dikarenakan syarat tidak terpenuhi kualifikasi dan proses selesai.

6. Teknisi memberikan informasi terkait dengan status hak akses yang diberikan pada pegawai baru melalui email ataupun secara langsung.
7. Setelah pegawai menerima informasi dari teknisi maka pegawai melakukan penandatanganan persetujuan hak akses.
8. Teknisi mengirimkan kepada pegawai ID, *password* dan mencatat pada *log* hak akses
9. Tahap pemberian hak akses pada sistem informasi yang dimiliki instansi dimulai dengan *login* pada panel *admin* yang sudah disediakan
    a. Masukkan *username* dan *password* teknisi
    b. Klik *login*
    c. Muncul tampilan form kode rahasia masukan kode rahasia teknisi
10. Setelah berhasil masuk pada panel *home*, pilih *menu setting user* setelah ikuti Langkah berikut sesuai dengan perubahan yang diinginkan:

10.1 Penambahan hak akses baru

a. Pilih menu tambah user (*New user*)
b. Muncul tampilan form isikan form tersebut
c. Masukkan nama
d. Masukkan NIP
e. Masukkan jabatan
f. Masukkan email
g. Pilih akses yang diminta
h. Setelah itu klik lanjutkan
i. Setelah itu pilih akses pada aplikasi yang diminta
j. Klik lanjutkan setelah itu muncul kolom kode aplikasi masukkan kode aplikasi
k. Klik simpan dan lanjutkan (*save* and *continue*) menunggu sampai muncul notifikasi penambahan user berhasil
l. Setelah itu muncul username dan *password* awal yang sesuai ketentuan

10.2 Perubahan hak akses

a. Pilih menu edit (edit user)
b. Muncul tampilan tabel user yang sudah terdaftar, pilih menu yang digantikan lalu klik edit
c. Muncul tampilan form yang sudah terisi, ganti isian form dengan user baru
d. Masukkan nama
e. Masukkan NIP
f. Masukkan jabatan

g. Masukkan *email*
h. Pilih akses yang diminta
i. Klik simpan dan lanjutkan menunggu sampai muncul notifikasi pergantian berhasil
j. Setelah itu muncul username dan *password* awal yang sesuai ketentuan

10.3 Penghapusan hak akses

a. Pilih menu hapus (*delete user*)
b. Muncul tampilan tabel user yang sudah terdaftar, pilih user yang dihapus lalu klik *delete*.
c. Muncul tampilan notifikasi pilih ya
d. Muncul tampilan form untuk kode rahasia masukkan kode rahasia teknisi klik simpan dan lanjutkan (*save and continue*)
e. Menunggu sampai muncul notifikasi penghapusan berhasil

3. RINCIAN INSTRUKSI KERJA

No.	Tanggal Revisi	Uraian Revisi

IK – 02. INSTRUKSI KERJA PERUBAHAN *PASSWORD*

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication* and *Technology* Department Head		
	IK 02	NO. RILIS	: 00
		NO. REVISI	: 00
	INSTRUKSI KERJA PERUBAHAN PASSWORD	TANGGAL TERBIT	:
		HALAMAN	:

1. PELAKSANA

Information Communication and *Technology* Department Head

2. RINCIAN INSTRUKSI KERJA

1. Kepala ICT menentukan standar pengguna *password* sesuai dengan kualitas *password* kuat
2. Kepala ICT meminta teknisi untuk menambahkan fitur *password* kuat untuk autentikasi *password*
3. Memastikan seluruh sistem yang membutuhkan prosedur log in telah memiliki inputan *password* kuat
4. Memasukkan fitur *password* kuat
    a. Jika berhasil maka seksi pengembangan aplikasi melakukan validasi *password* kuat, dan melakukan dokumentasi pelaporan dan pengisian form perbaikan sistem informasi
    b. Teknisi Analisa *password* kuat
5. Mempersiapkan prosedur lama dengan melakukan setup pada seluruh sistem
6. Menyediakan *password default* sementara yang sesuai dengan *password* untuk masing-masing pengguna
7. Melakukan *login* dengan menggunakan *password default*
8. Memastikan pegawai mengganti *password* default dengan kurun waktu yang telah ditentukan
9. Teknisi mengelola data *password* lama dan memastikan tidak ada pengguna/pegawai Kembali ke password default.
10. Tahap perubahan *password* pada sistem informasi yang dimiliki instansi dimulai dengan login ke sistem panel admin yang sudah disediakan

a. Masukkan username dan *password* lama
b. Klik login
c. Muncul tampilan form untuk *kode* rahasia masukkan kode rahasia teknisi

11. Setelah berhasil masuk pada panel home, pilih menu *setting password* setelah ikuti Langkah berikut sesuai dengan perubahan yang diinginkan:

11.1 Pemberian *password*

a. Pilih menu tambah *password*
b. Muncul tampilan form isikan form tersebut
c. Masukkan nama
d. Masukkan NIP
e. Masukkan jabatan
f. Masukkan *email*
g. Pilih akses yang diminta
h. Setelah itu klik lanjutkan
i. Setelah itu pilih akses pada aplikasi yang diminta
j. Klik lanjutkan setelah itu muncul kolom kode aplikasi masukkan kode aplikasi
k. Klik simpan muncul notifikasi penambahan user berhasil
l. Setelah itu muncul username dan *password* awal yang sesuai dengan ketentuan

11.2 Perubahan *Password*

a. Pilih menu edit
b. Muncul tampilan tabel *password* yang sudah terdaftar, pilih *password* yang digantikan lalu klik edit
c. Muncul tampilan form yang sudah terisi, ganti isian form dengan *password* baru
d. Masukkan nama
e. Masukkan NIP
f. Masukkan jabatan
g. Masukkan *email*
h. Pilih akses yang diminta
i. Klik simpan dan lanjutkan menunggu sampai muncul notifikasi pergantian berhasil
j. Setelah itu muncul username dan *password* awal yang sesuai ketentuan
k. Muncul tampilan ubah password awal dengan *password* baru
l. Setelah itu klik OK untuk menyimpan

11.3 Penghapusan *Password*

a. Pilih menu hapus
b. Muncul tampilan tabel *password* yang sudah terdaftar, pilih *password* yang dihapus lalu klik delete
c. Muncul tampilan notifikasi pilih ya
d. Muncul tampilan form untuk kode rahasia masukkan kode rahasia teknisi klik simpan dan lanjutkan
e. Menunggu sampai muncul notifikasi penghapusan berhasil.

3. RINCIAN INSTRUKSI KERJA

No.	Tanggal Revisi	Uraian Revisi

IK – 03. INSTRUKSI KERJA *RESET PASSWORD*

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication* and *Technology* Department Head		
	IK 03	NO. RILIS	: 00
		NO. REVISI	: 00
	INSTRUKSI KERJA *RESET PASSWORD*	TANGGAL TERBIT	:
		HALAMAN	:

1. PELAKSANA

Information Communication and *Technology Department Head*

2. RINCIAN INSTRUKSI KERJA

1. Mereset *password* pada sistem yang dimiliki perusahan dimulai dengan login pada panel *admin* yang sudah disediakan
   a. Masukkan *username* dan *password* teknisi
   b. Klik login
   c. Muncul tampilan form untuk kode rahasia masukkan kode rahasia teknisi
2. Setelah berhasil masuk pada panel home, pilih menu *management password*
3. muncul tampilan tabel yang berisikan user ID,nama,jabatan,divisi, hak akses, dan *password* (tampilan disembunyikan) pilih sesuai dengan pelapor
4. Klik *reset password*
5. Lalu muncul notifikasi untuk *mereset* password klik Ya
6. Setelah itu muncul *password* baru setelah direset

3. RINCIAN INSTRUKSI KERJA

No.	Tanggal Revisi	Uraian Revisi

IK – 04. INSTRUKSI KERJA *BACKUP* DATA DAN FILE

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication* and *Technology* Department Head		
	IK 04	NO. RILIS	: 00
		NO. REVISI	: 00
	INSTRUKSI KERJA *BACKUP* DATA DAN FILE	TANGGAL TERBIT	:
		HALAMAN	:

1. PELAKSANA

Seksi Pengelolaan Data

2. RINCIAN INSTRUKSI KERJA

1. *Backup database*
   a. Pastikan komputer terhubung dengan *server database oracle*, baik secara jaringan maupun secara teknisi
   b. *Install oracle* client pada PC
   c. *Setting tsnames*.ora
   d. Cek koneksi pada tsnames, buka cmd ketikkan, “tnsping ORCL11”(tanpa tanda titik)
   e. Jika proses berhasil maka muncul sedikit nilai mscc
   f. Setelah itu muncul lokasi hasil backup
      Set batfile : path file dimana kita menyimpan hasil backup *OracleDatabase*.
      Set batfile_log : *log* hasil *backup* data
   g. Simpan kode diatas dengan extensi.bat
   h. Kemudian jalankan file.bat tersebut dan tunggu hingga proses selesai
   i. Jika proses selesai, buka pada folder hasil *backup* muncul
      2 file dengan nama sesuai dengan setting batfile dan batfile_log.
   j. Ada file dengan ekstensi .dmp yang digunakan untuk *restore database* pada server

Nb : jika data yang dibackup berupa data kecil, menggunakan dump sql baik menggunakan aplikasi PLSQL Developer

3. RINCIAN INSTRUKSI KERJA

No.	Tanggal Revisi	Uraian Revisi

IK – 05. INSTRUKSI KERJA *RESTORE* DATA

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication* and *Technology Department Head*		
	IK 05	NO. RILIS	: 00
		NO. REVISI	: 00
	INSTRUKSI KERJA *RESTORE* DATA	TANGGAL TERBIT	:
		HALAMAN	:

1. PELAKSANA

Seksi Pengelolaan Data

2. RINCIAN INSTRUKSI KERJA

a. Mengaktifkan aplikasi PLSQL *Developer*
b. Login dengan menggunakan *Username* dan *password*
c. Jika sudah masuk dalam main screen pada PLSQL Developer selanjutnya pilih Tools > Import Tables
d. Klik Import
e. Pilih menu Tools > *Object* Browser kemudian klik pada menu tree Table

3. RINCIAN INSTRUKSI KERJA

No.	Tanggal Revisi	Uraian Revisi

IK – 06. INSTRUKSI KERJA PERAWATAN *HARDWARE*

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication* and *Technology Department Head*		
	IK 06	NO. RILIS	: 00
		NO. REVISI	: 00
	INSTRUKSI KERJA PERAWATAN *HARDWARE* DAN *JARINGAN*	TANGGAL TERBIT	:
		HALAMAN	:

1. PELAKSANA

Seksi Pemeliharaan Infrastruktur TI

2. RINCIAN INSTRUKSI KERJA

1. Pelaporan kerusakan *hardware*
   - 1.1 technical support/ teknisi melakukan pemeriksaan secara rutin alat-alat dalam kurun waktu sekali dalam satu minggu (4 kali dalam satu bulan)
   - 1.2 staff/pegawai membuat laporan lisan kepada staff seksi pemeliharaan teknologi informasi dan informasi bila terjadi kerusakan pada alat yang digunakan yang terjadi pada saat digunakan
   - 1.3 seksi pengendalian infrastruktur teknologi informasi dan komunikasi melakukan pengecekan *hardware* yang mengalami kerusakan
   - 1.4 staff seksi pengendalian teknologi informasi menyampaikan hasil pemeriksaan kerusakan alat kepada kepala ICT
   - 1.5 Dengan menyampaikan formulir laporan sistem informasi, dengan rekomendasi salah satu kerusakan pada formulir berita acara kerusakan yaitu sebagai berikut:
     a. Perbaikan material
     b. Pergantian material
   - 1.6 Staff seksi pengendalian infrastruktur TIK melakukan pencatatan dokumentasi pada formulir laporan evaluasi pengguna perangkat TI
2. Perbaikan *hardware*
   - 2.1 kepala bidang infrastruktur Teknologi Informasi dan Komunikasi memutuskan untuk memperbaiki alat berdasarkan laporan uraian perbaikan,

analisis/tinjauan pada formulir laporan perbaikan sistem informasi, dan formulir berita acara kerusakan

2.2 kepala bidang infrastruktur Teknologi Informasi dan Komunikasi memutuskan untuk memperbaiki alat berdasarkan laporan uraian perbaikan, analisis/tinjauan pada formulir laporan perbaikan sistem informasi, dan formulir berita acara kerusakan

2.3 setelah perbaikan atau pergantian material *hardware* selesai staff seksi pemeliharaan infrastruktur TI melakukan pencatatan laporan kerusakan hardware pada formulir pemeliharaan perangkat TI

2.4 hardware telah diperbaiki dan Kembali fungsinya seperti semula dan dapat digunakan Kembali

2.5 staff pengendalian infrastruktur TI melakukan pelaporan validasi formulir pemeliharaan TI.

2.6 Melakukan pengisian dan mendokumentasikan laporan perbaikan *hardware* kepada kepala ICT.

3. Pemeliharaan *hardware*

3.1 Staff pemeliharaan infrastruktur TI melakukan pemeliharaan *hardware* sesuai denga napa yang dilaporkan

3.2 Mencatat kegiatan pemeliharaan *hardware* pada formulir pemeliharaan perangkat TI

3.3 Memastikan *hardware* dapat digunakan dengan maksimal

3.4 Melaporkan kepada staff pengendalian infrastruktur TI melakukan pelaporan validasi formulir pemeliharaan TI

3.5 Melakukan pengisian dan mendokumentasikan laporan pengelolaan perangkat TI kepada kepala ICT.

3. RINCIAN INSTRUKSI KERJA

No.	Tanggal Revisi	Uraian Revisi

IK – 07. INSTRUKSI KERJA PERAWATAN KABEL DAN JARINGAN TELEKOMUNIKASI

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication* and *Technology* Department Head		
	IK 07	NO. RILIS	: 00
		NO. REVISI	: 00
	INSTRUKSI KERJA PERAWATAN KABEL	TANGGAL TERBIT	:
		HALAMAN	:

1. PELAKSANA

Seksi Pemeliharaan Infrastruktur TI

2. RINCIAN INSTRUKSI KERJA

1. Pemeliharaan kabel jaringan telekomunikasi
   1.1. Staff seksi jaringan infrastruktur TI melakukan pemeliharaan kabel jaringan telekomunikasi sesuai denga napa yang dilaporkan
   1.2. Mencatat kegiatan pemeliharaan kabel jaringan telekomunikasi
   1.3. Memastikan kabel jaringan telekomunikasi dapat digunakan dengan maksimal
   1.4. Melaporkan kepada staff seksi jaringan infrastruktur TI melakukan pelaporan validasi formulir pemeliharaan TI.
   1.5. Melakukan pengisian dan mendokumentasikan laporan pengelolaan perangkat TI kepada kepala ICT.
2. Pelaporan kerusakan kabel jaringan telekomunikasi
   2.1 *Technical support*/teknisi melakukan pemeriksaan secara rutin alat-alat dalam kurun waktu sekali dalam satu minggu (4 kali dalam satu bulan) pelaporan kerusakan kondisi fisik perangkat hardware.
   2.2 Staff/pegawai membuat laporan lisan kepada staff seksi pemeliharaan teknologi informasi dan informasi bila terjadi kerusakan pada alat yang digunakan yang terjadi pada saat digunakan
   2.3 Seksi pengendalian infrastruktur teknologi informasi dan komunikasi melakukan pengecekan hardware yang mengalami kerusakan
   2.4 Staff seksi pengendalian teknologi informasi menyampaikan hail pemeriksaan kerusakan alat kepada kepala ICT dengan menyampaikan formulir laporan

perbaikan sistem informasi, dengan rekomendasi salah satu kerusakan pada formulir berita acara kerusakan yaitu sebagai berikut:

a. Perbaikan material
b. Pergantian material

2.5 Staff seksi pengendalian infrastruktur TIK melakukan pencatatan dokumentasi pada formulir laporan evaluasi penggunaan perangkat TI.

3. Perbaikan kabel jaringan telekomunikasi

3.1 Staff seksi pengendalian infrastruktur TIK memutuskan untuk memperbaiki alat berdasarkan laporan uraian perbaikan, analisis/tinjauan pada formulir laporan perbaikan sistem informasi dan formulir berita acara kerusakan.

3.2 Seksi pemeliharaan infrastruktur TI melakukan perbaikan dan melakukan pencatatan perbaikan pada formulir pemeliharaan perangkat TI

3.3 Setelah perbaikan atau pergantian hardware selesai staff seksi pemeliharaan infrastruktur TI melakukan pencatatan laporan kerusakan hardware pada formulir pemeliharaan perangkat TI

3.4 *Hardware* telah diperbaiki dan Kembali fungsinya seperti semula dan dapat digunakan Kembali

3.5 Staff pengendalian infrastruktur TI melakukan pelaporan validasi formulir pemeliharaan TI

3.6 Melakukan pengisian dan mendokumentasikan laporan perbaikan *hardware* kepada kepala ICT.

3. RINCIAN INTRUKSI KERJA

No.	Tanggal Revisi	Uraian Revisi

IK – 08. INSTRUKSI KERJA PELATIHAN DAN PENGEMBANGAN SDM

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT Sekretariat		
	IK 08	NO. RILIS	: 00
		NO. REVISI	: 00
	INSTRUKSI KERJA PELATIHAN DAN PENGEMBANGAN SDM	TANGGAL TERBIT	:
		HALAMAN	:

1. PELAKSANA

Sekretariat

2. RINCIAN INSTRUKSI KERJA

1. Proses Pendaftaran Pengembangan dan Pelatihan

1.1. Pegawai membuat permintaan pendaftaran kegiatan

1.2. Pegawai meminta kesekretariatan untuk membuat permohonan keikut sertaan kegiatan tersebut

1.2.1 jika pengajuan permohonan disetujui oleh staff bagian kesekretariatan, maka proses dilanjutkan pada memberikan informasi mengenai kegiatan pengembangan kompetensi yang diadakan.

1.2.2 jika pengajuan permohonan tidak disetujui maka proses Kembali pada sub-proses 1.2

2. Proses persiapan pengembangan dan Pelatih
    2.1 Staff persiapan pelatihan dan pengembangan oleh kesektretariatan menyiapkan kegiatan tersebut dengan apa yang telah ditentukan
    2.2 Staff kesekretariatan memberikan surat tugas kepada pegawai untuk keikut sertaannya dalam kegiatan pelatihan dan pengembangan.
3. Proses Pengembangan dan pelatihan
    3.1 Pegawai/peserta pelatihan dan pengembangan hadir ditempat
    3.2 Peserta/pegawai melakukan presensi pada formulir data pegawai yang telah di sediakan oleh staff sekretariat
    3.3 Sekretariat melakukan pencatatan kegiatan pelatihan dan pengembangan dan catatan data peserta pada formulir data pegawai.
4. Evaluasi Pengembangan dan Pelatihan
    4.1 Bagian sekretariat membuat laporan sebagai pertanggung jawaban kepada pihak kepala bidang
    4.2 Laporan pertanggung jawaban kegiatan pelatihan dan pengembangan yang telah dibuat oleh sekretariat diberikan kepada kepala bidang
    4.3 Pegawai/peserta melakukan evaluasi menggunakan formulir evaluasi kegiatan pengembangan kompetensi setelah selesainya kegiatan pelatihan dan pengembangan
    4.4 Sekretariat melakukan percakapan penilaian dalam kegiatan pelatihan dan pengembangan, guna mempertimbangkan penilaian tahunan untuk pegawai

3. RINCIAN INSTRUKSI KERJA

No.	Tanggal Revisi	Uraian Revisi

IK – 09. INSTRUKSI KERJA KLASIFIKASI KEAMANAN INFORMASI

Angkasa Pura | AIRPORTS	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication* and *Technology Department Head*		
	IK 09	NO. RILIS	: 00
		NO. REVISI	: 00
	INSTRUKSI KERJA KLASIFIKASI KEAMANAN INFORMASI	TANGGAL TERBIT	:
		HALAMAN	:

1. PELAKSANA

Information Communication and *Technology Department Head*

2. RINCIAN INSTRUKSI KERJA

1. Klasifikasi keamanan informasi
   1.1. Sekretaris melakukan pengklasifikasian data yang dijadikan informasi bagi yang membutuhkan
   1.2. Klasifikasi data tersebut di dapatkan dari staff data komunikasi dan dilakukan pengklasifikasian agar memudahkan dalam penyampaian informasi
   1.3. Pembuatan informasi
   1.4. Informasi yang disebarkan harus terotorisasi oleh staff persandian dan keamanan informasi agar tidak terjadi penyalahgunaan dalam penyampaian dan pemanfaatan informasi tersebut
   1.5. Staff keamanan dan persandian melakukan monitoring informasi yang di publish apakah sudah sesuai atau belum:
      a. Jika informasi yang disampaikan sudah memenuhi standar untuk dilakukan pempublikasian maka informasi siap di publish dan staff harus melakukan pengisian dalam form monitoring informasi
      b. Jika informasi belum memenuhi standar pembuatan informasi maka informasi harus diperbaiki agar memenuhi standar pada bagian klasifikasi data informasi guna melengkapi proses pembuatan informasi.

3. RINCIAN INSTRUKSI KERJA

No.	Tanggal Revisi	Uraian Revisi

IK – 10. INSTRUKSI KERJA PERAN DAN TANGGUNG JAWAB KEAMANAN INFORMASI

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication* and *Technology Department Head*		
	IK 10	NO. RILIS	: 00
		NO. REVISI	: 00
	INSTRUKSI KERJA PERAN DAN TANGGUNG JAWAB KEAMANAN INFORMASI	TANGGAL TERBIT	:
		HALAMAN	:

1. PELAKSANA

Information Communication and *Technology Department Head*

2. RINCIAN INSTRUKSI KERJA

1. Peran dan tanggung jawab keamanan informasi
   1.1. Sekretaris memberikan peran dan tanggung jawab untuk informasi sesuai dengan yang disampaikan dan sesuai dengan tugas staff masing-masing
   1.2. Penandatanganan peran dan tanggung jawab
   1.3. Informasi siap untuk dipublikasikan
   1.4. Proses monitoring informasi dilakukan oleh yang bertanggung jawab dan mendokumentasikannya dalam form monitoring informasi yang ada serta membuat laporan monitoring informasi kepada kepala ICT

3. RINCIAN INSTRUKSI KERJA

No.	Tanggal Revisi	Uraian Revisi

LAMPIRAN 14

HASIL PERENCANAAN FORMULIR

FM – 01. FORMULIR PENGELOLAAN HAK AKSES

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication and Technology Department Head*		
	FM 01	NO. RILIS	: 00
		NO. REVISI	: 00
	FORMULIR PENGELOLAAN HAK AKSES	TANGGAL TERBIT	: 00
		HALAMAN	: 01
FORMULIR			

Tanggal : *(Diisi tanggal pengajuan pengendalian hak akses)*

Waktu : *(Diisi pada pukul jam berapa formulir diajukan)*

Status : *(Diisi status saat ini hak akses)*

JENIS PENGELOLAAN HAK AKSES	SALURAN
☐ **Pemberian Hak akses** ☐ **Penghapusan Hak Akses** ☐ **Perubahan Hak akses** *(centang yang perlu)*	☐ ***E-mail*** ☐ **Telepon** ☐ ***Offline*** *(centang yang perlu)*
IDENTITAS PEGAWAI	
Nama Pegawai	*(nama lengkap pegawai)*
NIP	*(Nip Pegawai)*
Jabatan	*(keterangan jabatan pegawai)*
Email	*(email pegawai)*
No.Hp	*(Diisi no.Hp Pegawai)*
PERMINTAAN HAK AKSES	JENIS APLIKASI
Akses Saat ini : *(centang yang perlu)* ☐ **Teknisi** ☐ **ICT** ☐ ***Airport Technology, network, operation suppoer section head*** ☐ ***General Manager***	☐ **FIDS** ☐ ***Counter check-in*** *(centang yang perlu)*
CATATAN :	
Disetujui Oleh : *(ttd)*	Diketahui Oleh : *(ttd)*

FM – 02. KONTRAK PERJANJIAN HAK AKSES

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication and Technology Department Head*	
	FM 02	NO. RILIS : 00
		NO. REVISI : 00
	FORMULIR KONTRAK PERJANJIAN HAK AKSES	TANGGAL TERBIT : 00
		HALAMAN : 01/03
FORMULIR		

PERJANJIAN KERAHASIAAN ATAS HAK AKSES PT ANGKASA PURA 1 SURABAYA

Nomor :

Perjanjian kerahasiaan atas hak akses yang ada di PT Angkasa Pura 1 Surabaya, Selanjutnya disebutkan perjanjian kerahasiaan, dibuat pada hari ini,……Tanggal……bulan……tahun……di…… *(lokasi)*, oleh dan antara :

1. Nama:
   Jabatan :
   Dalam hal ini disebut sebagai PIHAK PERTAMA yang bertindak sebagai penanggung jawab pemberian hak akses
   Nama:
   Jabatan :
   Dalam hal ini disebut sebagai PIHAK KEDUA yang bertindak sebagai penanggung jawab pemberian hak akses

PASAL 1

Informasi Rahasia

1.1. Untuk kepentingan perjanjian ini definisi dari “Informasi Rahasia” adalah sebagai berikut :

1.1.1. Setiap informasi mengenai atau yang berhubungan dengan PT Angkasa Pura 1 Surabaya, badan instansi lain dan kegiatan operasionalnya yang disampaikan atau diungkapkan oleh pemberi informasi kepada penerima informasi atau

masyarakat, pihak internal instansi baik secara lisan, tulisan, grafik, elektronik, atau dalam bentuk lain, baik langsung maupun tidak langsung

1.1.2. Setiap informasi mengenai atau yang berhubungan dengan transaksi, ketentuan transaksi, perjanjian yang mengatur transaksi, ketentuan perjanjian yang mengatur transaksi dan setiap dokumen yang terkait dengan transaksi yang diberikan secara langsung maupun tidak langsung, oleh pemberi kepada penerima sehubungan dengan atau hal terkait dengan transaksi; atau

1.1.3. Segala komunikasi antara para pihak, baik secara lisan maupun yang diketahui atau semestinya diketahui oleh para pihak untuk menjadi rahasia atau menjadi milik instansi secara alami, dan yang dibuat dalam rangkaian diskusi atau pekerjaan lain yang dilakukan antara para pihak

1.2. Informasi rahasia tidak termasuk “Informasi yang tidak dilindungi” sebagaimana dijelaskan dalam pasal 2 perjanjian ini.

PASAL 2

Informasi yang tidak Dilindungi

Untuk kepentingan perjanjian ini, yang dimaksud dengan “Informasi yang tidak dilindungi” adalah sebagai berikut:

1.1. Informasi yang pada saat penyampaiannya atau pengungkapannya, sudah berada pada kepemilikan yang sah dari penerimaan atau tersedia pada penerima dari sumber lain yang tidak memiliki kewajiban untuk tidak menyampaikan atau mengungkapkan; atau

1.2. Informasi yang merupakan, atau setiap saat ini menjadi, tersedia untuk umum selain dari pelanggaran perjanjian ini oleh penerima.

PASAL 3

Lingkup Perjanjian

2.1. penerima setuju untuk setiap saat:

2.1.1 tidak mengungkapkan informasi rahasia kepada pihak manapun

2.1.2 mengambil seluruh Tindakan yang diperlukan untuk melindungi kerahasiaan dan informasi rahasia; dan informasi atau masyarakat, pihak instansi baik secara lisan, tulisan, grafik, elektronik, atau dalam bentuk lain, baik langsung maupun tidak langsung

2.1.3 setiap informasi mengenai atau yang berhubungan dengan transaksi ketentuan transaksi, perjanjian yang mengatur transaksi, ketentuan perjanjian yang mengatur transaksi dan setiap dokumen yang terkait dengan transaksi yang diberikan secara langsung maupun tidak langsung, oleh pemberi kepada penerima sehubungan dengan atau hal terkait dengan transaksi; atau

2.1.4 segala komunikasi antara para pihak, baik secara lisan maupun yang diketahui atau semestinya diketahui oleh para pihak untuk menjadi kerahasiaan atau menjadi milik instansi secara alami, dan yang dibuat dalam rangkaian diskusi atau pekerjaan lain yang dilakukan antara para pihak.

2.1.5 Menghindari pengungkapan atau penyalahgunaan dari informasi rahasia

Demikian perjanjian kerahasiaan atas hak akses ini dibuat dan ditandatangani oleh PIHAK PERTAMA dan PIHAK KEDUA ditempat dan pada tanggal tersebut diatas, dalam rangkap 2 (dua) asli bermaterai cukup, masing-masing pihak telah menandatangani perjanjian ini melalui wakil yang ditunjuk.

PIhak Pertama		**Pihak Kedua**	
Tanda Tangan	:	Tanda Tangan:	
Dicetak Nama	:	Dicetak Nama	:

FM – 03. FORMULIR *LOG* PENGELOLAAN HAK AKSES

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication and Technology Department Head*		
	FM 01	NO. RILIS	: 00
		NO. REVISI	: 00
	FORMULIR LOG PENGELOLAAN HAK AKSES	TANGGAL TERBIT	: 00
		HALAMAN	: 01
FORMULIR			

No	NIP	Nama Pegawai	Tanggal	Jam	Jenis Akses	Status Verifikasi
	(NIP Pegawai)	*(Nama Lengkap Pegawai)*	*(Tanggal Pengajuan Log Pengelolaan Hak Akses)*	*(Jam Pengajuan)*	*(jenis akses apa yang diajukan)*	☐
						☐
						☐
						☐
						☐
						☐
						☐

Keterangan :

- Status verifikasi diisi tanda centang (√) apabila telah terverifikasi dan tanda silang (×) apabila belum terverifikasi.

FM – 04. FORMULIR PERBAIKAN SISTEM INFORMASI

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication and Technology Department Head*		
	FM 04	NO. RILIS	: 00
		NO. REVISI	: 00
	FORMULIR PERBAIKAN SISTEM INFORMASI	TANGGAL TERBIT	: 00
		HALAMAN	: 01
FORMULIR			

Laporan Perbaikan Sistem Informasi

Tanggal……Bulan……Tahun……

Tanggal	*(tanggal permintaan perbaikan sistem)*	Pukul	
Nama	*(nama pihak terkait yang melakukan permintaan perbaikan sistem)*		
Unit Kerja	*(unit kerja terkait yang melakukan permintaan perbaikan sistem)*		
Menu & Submenu yang diperbaiki	*(keterangan menu/sub menu fitur)*		
Uraian Perbaikan	*(keterangan perbaikan sistem informasi)*		
REALISASI KERJA			
Analisis/Tinjauan *(diis oleh pengembang aplikasi)*	*(keterangan analisis perbaikan sistem informasi yang dilakukan)*		
Perbaikan *(diisi oleh pengembang aplikasi)*	*(keterangan perbaikan sistem informasi yang dilakukan)*		
Tanggal Mulai	*(tanggal mulai perbaikan sistem informasi)*	Pukul	
Tangal Selesai	*(tanggal berkahir perbaikan sistem informasi)*	Pukul	
Mengetahui, Kepala ICT (*Nama Lengkap*) NIP ……	*(Lokasi, tanggal, bulan, Tahun)* Teknisi (*nama lengkap*) NIP ……..		

FM – 05. FORMULIR PERMINTAAN *RESET* PASSWORD

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication and Technology Department Head*	
	FM 05	NO. RILIS : 00
		NO. REVISI : 00
	FORMULIR PERMINTAAN *RESET* PASSWORD	TANGGAL TERBIT : 00
		HALAMAN : 01
FORMULIR		

FORMULIR PERMINTAAN *RESET* PASSWORD Nomor FM-05-..../...../...../.....	
Pemohon	
Tanggal : *(tanggal permintaan reset password)*	Tanda Tangan :
Nama : *(Nama lengkap pegawai)*	
NIP : *(NIP pegawai)*	
Jabatan : *(keterangan jabatan pegawai)*	
Staff/Seksi : *(keterangan staff/seksi yang disetujui)*	(*Nama Lengkap Pemohon*) NIP ……
Email aktif : *(email pegawai)*	
Keterangan *(diisi dengan alasan permintaan reset password)*	
(Lokasi, tanggal, bulan, tahun) Teknisi, *(Nama lengkap pegawai)* NIP ……..	

FM – 06. FORMULIR KLASIFIKASI DATA

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication and Technology Department Head*		
	FM 06	NO. RILIS	: 00
		NO. REVISI	: 00
	FORMULIR KLASIFIKASI DATA	TANGGAL TERBIT	: 00
		HALAMAN	: 01
FORMULIR			

FORMULIR KLASIFIKASI DATA

Periode ……..Tahun……..

No.	Jenis Data	Klasifikasi	Kritikalisasi
1.	Data Keuangan	*rahasia*	*Tinggi*
	a. Total anggaran perbulan	*rahasia*	*Tinggi*
	b. Total anggaran pertahun		
2.	(klasifikasi kelompok Data)		
	a. (data)	*(Klasifikasi)*	*(kritikalisasi)*
	b. (data)	*(Klasifikasi)*	*(kritikalisasi)*
	c. (data)	*(Klasifikasi)*	*(kritikalisasi)*
	d. (data)	*(Klasifikasi)*	*(kritikalisasi)*
3.	Klasifikasi kelompok (Data)		
	a. (data)	*(Klasifikasi)*	*(kritikalisasi)*
	b. (Data)	*(Klasifikasi)*	*(kritikalisasi)*
	c. (Data)	*(Klasifikasi)*	*(kritikalisasi)*
4.	Klasifikasi kelompok (Data)		
	a. (Data)	*(Klasifikasi)*	*(kritikalisasi)*
	b. (Data)	*(Klasifikasi)*	*(kritikalisasi)*
	c. (Data)	*(Klasifikasi)*	*(kritikalisasi)*
Dst.			

(lokasi, Tanggal, bulan tahun)

Teknisi,

(*Nama Lengkap*)

NIP……..

FM – 07 FORMULIR *LOG BACK-UP* DATA

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication and Technology Department Head*	
	FM 07	NO. RILIS : 00
		NO. REVISI : 00
	FORMULIR *LOG BACK-UP DATA*	TANGGAL TERBIT : 00
		HALAMAN : 01
FORMULIR		

LOG BACK-UP SHEET

Bulan ……..Tahun……..

Log ke-	*1*	*11*	*111*	*1V*	*Dst…*
Tanggal *(1)*					
Waktu *(2)*					
Metode *(3)*					
Jumlah media *(4)*					
Mana media *backup (5)*					
Isi media *backup (6)*					
Status *backup (7)*					
Keterangan *(8)*					

Keterangan pengisian :

(1)Diisi dengan tanggal *backup*

(2)Diiisi dengan waktu *bckup* berhasil dilakukan (*backup complete)*

(4)Diisi dengan jumlah media *backup*

(5)Diisi dengan nama media backup

(6)Diisi dengan keterangan data file dalam media *backup*

(7)Diisi dengan status *backup*

(8)Diisi dengan keterangan dari status *Backup* data yang berhasil/data yang tidak di *Backup, eror yang terjadi dll.*

(lokasi, Tanggal, Bulan, Tahun)

Teknisi,

(Nama Lengkap)

NIP……

FM – 08. FORMULIR *RESTORE* DATA

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication and Technology Department Head*		
	FM 08	NO. RILIS	: 00
		NO. REVISI	: 00
	FORMULIR *RESTORE* DATA	TANGGAL TERBIT	: 00
		HALAMAN	: 01
FORMULIR			

RESTORE DATA	
Tanggal *Backkup*	*(tanggal melakukan backup data)*
Nama Staff	*(nama pegawai yang melakukan restore data)*
Sumber Data	*(keterangan terkait sumber backup)*
Data yang di restore	*Keterangan terkait data yang di resttoe*
Tipe *Backup*	Full backup *Partial/Incremental* Backup
Media *Backup*	*(media yang digunakan untuk penyimpanan data backup)*
Recovery point of objective	*Keterangan bagian data yang direstore setelah pemulihan layanan teknologi informasi)*
Catatan	
(Lokasi, Tanggal, bulan, Tahun) Teknisi, (nama lengkap pegawai) NIP ……..	

FM – 09. FORMULIR PEMELIHARAAN PERANGKAT TI

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication and Technology Department Head*		
	FM – 09	NO. RILIS	: 00
		NO. REVISI	: 00
	FORMULIR PEMELIHARAAN PERANGKAT TI	TANGGAL TERBIT	: 00
		HALAMAN	: 01
FORMULIR			

No. Form : *(nomor form pemeliharaan perangkat TI)*
Tanggal : *(tanggal pengajuan pemeliharaan)*

Jenis Perangkat TI : *(jenis perangkat yang dilakukan pemeliharaan)*
Jumlah : *(jumlah perangkat yang dilakukan pemeliharaan)*

Pemeliharaan yang dilakukan :

(Log aktivitas pemeliharaan yang dilakukan)

Tanggal Pemeliharaan	Waktu	Pelaksanaan	Keterangan
(tanggal pemeliharaan)	*(waktu pemeliharaan)*	*(pelaksanaann pemeliharaan perangkat TI)*	*(keterangan pemeliharaan perangkat TI)*

Diketahui Oleh,
Kepala Bidang Infrastruktur TI

(*Nama Lengkap kepala bagian Infrastruktur TI*)
NIP …….

(lokasi, tanggal, bulan, tahun)
Pegawai yang bertugas,

(*nama pegawai*)
NIP …….

FM – 10. FORMULIR BERITA ACARA KERUSAKAN

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication and Technology Department Head*	
	FM 10	NO. RILIS : 00
		NO. REVISI : 00
	FORMULIR BERITA ACARA KERUSAKAN	TANGGAL TERBIT : 00
		HALAMAN :
FORMULIR		

No. Form : *(nomor formulir berita acara kerusakan)*
No. Berita Acara : *(nomor, berita acara)*
Tanggal : *(tanggal berita acara dibuat)*

Kerusakan : *(centang yang perlu)*

- ☐ PC
- ☐ Komputer
- ☐ Router/Hub
- ☐ Wireless
- ☐ LCD/Proyekto
- ☐ Kabel Telekomunikasi
- ☐ Printer/Scanner

Penyebab Kerusakan :

(tuliskan penyebab kerusakan)

Perbaikan / Pergantian Material :
Nama Barang : *(nama barang yang di perbaiki)*
Type : *(type barang yang diperbaiki)*
S/N : *(isi kondisi material S= second, N=New)*
Jumlah : *(jumlah perbaikan atau material)*

Tanggal Pemeliharaan	Waktu	Pelaksanaan	Keterangan
(tanggal pemeliharaan)	*(waktu pemeliharaan)*	*(pelaksanaan pemeliharaan perangkat TI)*	*Keterangan pemeliharaan perangkat TI)*

Diketahui Oleh, Kepala Bidang Infrastruktur TI *(Nama Lengkap)* NIP ……..	*(lokasi, tanggal, bulan, tahun)* Pengguna *(nama lengkap)* NIP……

FM – 11. FORMULIR LAPORAN EVALUASI PENGELOLAAN PERANGKAT TI

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication and Technology Department Head*	
	FM 11	NO. RILIS : 00
		NO. REVISI : 00
	FORMULIR LAPORAN EVALUASI PENGELOLAAN PERANGKAT TI	TANGGAL TERBIT : 00
		HALAMAN :
FORMULIR		

No.	Jenis Perangkat	Kerusakan	Tanggal Kerusakan	Tanggal Pemeliharaan	Keterangan	Pegawai yang bertugas
	(jenis perangkat yang dilakukan pengelolaan)	*(Jenis Kerusakan)*	*(Tanggal, Bukan, Tahun)*	*(Tanggal, bulan, tahun)*	*(Status keterangan)*	*()Nama Pegawai*

(lokasi, tanggal, bulan, tahun)

Diketahui Oleh,

Kepala Bidang Pengelolaan Data dan Statistika

(Nama Lengkap Kepala Bidang)

NIP …….

FM – 12. FORMULIR DATA PEGAWAI

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication and Technology Department Head*	
	FM 12	NO. RILIS : 00
		NO. REVISI : 00
	FORMULIR DATA PEGAWAI	TANGGAL TERBIT : 00
		HALAMAN :
FORMULIR		

FORMULIR KEHADIRAN PEGAWAI

Tanggal : *(tanggal kehadiran)* Instruktur : *(nama pembicara)*

Topik : *(topik pembahasan* Tempat : *(Tempat penyelenggaraan)*

No.	Nama Pegawai	Bidang	Jabatan	Tanda Tangan	Keterangan
	(Nama Lengkap pegawai)	*(bidang pada*	*(jabatan pegawai)*	*(tanda tangan pegawai*	*(keterangan kehadiran)*

(Lokasi, tanggal, bulan, tahun)

Kasubag Tata Usaha

(Nama lengkap Kasubag)

NIP …….

FM – 13. FORMULIR EVALUASI KEGIATAN PENGEMBANGAN KOMPETENSI

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication and Technology Department Head*	
	FM – 13	NO. RILIS : 00
		NO. REVISI : 00
	FORMULIR EVALUASI KEGIATAN PENGEMBANGAN KOMPETENSI	TANGGAL TERBIT : 00
		HALAMAN :
FORMULIR		

FORMULIR EVALUASI PELATIHAN

Nama : *(nama lengkap pegawai)* Bidang : *(bidang pada instansi* Judul Materi : *(judul materi yang dibawakan*	Jabatan : *(jadwal pegawai)* Seksi : *(seksi pegawai pada instansi)* Tgl Pelatihan : (tanggal, bulan, tahun pelatihan)
Sasaran Pelatihan : *(sasaran pelatihan)*	
Evaluasi Pelatihan : *(centang yang perlu)* ☐ Langsung setelah pelatihan ☐ 1 Bulan setelah pelatihan ☐ 2 bulan setelah pelatihan ☐ 3 bulan setelah pelatihan ☐ Lain-lain ……..	
Metode Evaluasi : *(centang yang perlu)* ☐ Tes/Ujian ☐ Observasi/Pengamatan	
Point Evaluasi : *(lingkari huruf sesuai penilaian)* ☐ **Pengetahuan** Mampu menjelaskan isi /materi training **Y - N** Mampu menjelaskan konsep-konsep yang ada pada training **Y - N**	

☐ **Sikap** *(lingkari huruf sesuai penilaian)* Menunjukkan sikap sesuai dengan konsep dari training	**Y - N** **Y - N**
☐ **Keterampilan** *(dapat melakukan keterampilan seperti yang diajarakan dalam pelatihan) (lingari hruf sesuai penilaian)* 1. ……. 2. ……. 3. ……. 4. ……. 5. …….	 **Y - N** **Y - N**
Tindak lanjut dari evaluasi : *(isikan saran dan tindak lanjut untu evaluasi)* ……..	

Diketahui Oleh, *(lokasi, tanggal, bulan, tahun)*

Kepala Bidang Pengelolaan Data dan Statistika Diketahui oleh,

(Nama Lengkap Kepala bidang) *(Nama Lengkap seksi evaluasi dan informasi)*

NIP …….. NIP …….

FM – 14. FORMULIR MONITORING KEAMANAN INFORMASI

	INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT *Information Communication and Technology Department Head*		
	FM 14	NO. RILIS	: 00
		NO. REVISI	: 00
	FORMULIR *MONITORING* KEAMANAN INFORMASI	TANGGAL TERBIT	:
		HALAMAN	: 01
FORMULIR			

FORMULIR MONITORING KEAMANAN INFORMASI

Periode …… Tahun ……

No.	Jenis Informasi	Klasifkasi	Monitoring
1.	Informasi internal		
	a. Surat pegawai	*(rahasia)*	*(berhasil)*
	b.	*(rahasia)*	*(gagal)*
	c.		
	d.		
2.	Informasi Publik		
	a. (Informasi)	*(klasifikasi)*	*(monitoring)*
	b. (Informasi)	*(klasifikasi)*	*(monitoring)*
	c. (Informasi)	*(klasifikasi)*	*(monitoring)*
	d. (Informasi)	*(klasifikasi)*	*(monitoring)*
3.	(klasifikasi kelompok informasi)		
	a. (Informasi)	*(klasifikasi)*	*(monitoring)*
	b. (Informasi)	*(klasifikasi)*	*(monitoring)*
	c. (Informasi)	*(klasifikasi)*	*(monitoring)*
	d. (Informasi)	*(klasifikasi)*	*(monitoring)*
Dst.			

(lokasi, tanggal, bulan tahun)
Staff Bidang

(*Nama Lengkap*)
NIP ……

DAFTAR RIWAYAT HIDUP

NAMA	: Yusuf Bahrudin Nizar
NIM	: 15.41010.0185
Tempat Lahir	: Temanggung
Tanggal Lahir	: 20, Januari 1997
Agama	: Islam
Alamat	: Perumtas 3 blok e5 no 4 RT: 042 RW: 006, Kec Tulangan – Sidoarjo.
Telepon	: 081230707932
Email	: Yusufbahrudin97@gmail.com

Riwayat Pendidikan

2003 – 2009	SDN Kramat Jegu I
2009 – 2012	SMPN I Tlogomulyo
2012 – 2015	SMA Antartika Sidoarjo

Perguruan Tinggi

Program Studi	: Sistem Informasi
Fakultas	: Teknologi dan Informatika
Nama Perguruan Tinggi	: Universitas Dinamika
Kota perguruan Tinggi	: Surabaya