PUSRI
PUPUK SRIWIDJAJA PALEMBANG

PUPUK INDONESIA HOLDING COMPANY

"S A L I N A N"

SURAT KEPUTUSAN DIREKSI
PT PUPUK SRIWIDJAJA PALEMBANG
NOMOR : SK/DIR/430/2023

tentang,

PEDOMAN PENGELOLAAN KEAMANAN INFORMASI
PT PUPUK SRIWIDJAJA PALEMBANG

Direksi PT Pupuk Sriwidjaja Palembang,

Menimbang :

a. bahwa penerapan Sistem Manajemen Keamanan Informasi perlu dilengkapi dengan ketentuan dan panduan dalam pengimplementasiannya guna tercapai sasaran penerapan sistem manajemen yang efektif dan berkelanjutan;

b. bahwa untuk meningkatkan efektivitas proses pengelolaan keamanan informasi tersebut diperlukan ketentuan atau pedoman yang mengatur pelaksanaannya;

c. bahwa untuk tertib administrasi, perlu ditetapkan dengan Surat Keputusan Direksi;

Mengingat :

1. Akta Nomor 14 tanggal 12 November 2010 tentang Pendirian Perseroan Terbatas PT Pupuk Sriwidjaja Palembang yang dibuat dihadapan Fathiah Helmi, S.H., Notaris di Jakarta, sebagaimana telah beberapa kali diubah dan terakhir diubah dengan Akta Nomor 01 tanggal 02 November 2022 tentang Pernyataan Keputusan Pemegang Saham PT Pupuk Sriwidjaja Palembang yang dibuat di hadapan Notaris Imelda Sugiharti, S.H., M.Kn., Notaris di Palembang;
2. Akta Nomor 03 tanggal 13 November 2023 tentang Berita Acara Rapat Umum Pemegang Saham Luar Biasa PT Pupuk Sriwidjaja Palembang yang dibuat dihadapan Lumassia, S.H., Notaris di Jakarta;
3. Akta Nomor 05 tanggal 25 Februari 2021 tentang Pernyataan Keputusan Pemegang Saham PT Pupuk Sriwidjaja Palembang tentang Pengangkatan Anggota Direksi yang dibuat dihadapan Lumassia, S.H., Notaris di Jakarta;
4. Perjanjian Bersama antara Perusahaan dengan Anak Perusahaan Nomor 209/A/HK/A21/SP/2020, Nomor 1475/B/HK.01.01/13/SP/2020, Nomor 520/PK/SP/UK/XI/2020, Nomor 10610/SP-BTG/2020, Nomor 196/SP/DIR/PIM/LSM/2020, Nomor 265/SP/DIR/2020 tanggal 9 November 2020 Tentang Implementasi Kewenangan PT Pupuk Indonesia (Persero) Sehubungan Dengan Penyelenggaraan Fungsi/Bidang Tertentu Untuk Anak Perusahaan;
5. Surat Keputusan Direksi PT Pupuk Sriwidjaja Palembang Nomor: SK/DIR/438/2020 tanggal 30 Desember 2020 tentang Pengesahan Pedoman PT Pupuk Indonesia (Persero) Terhadap Fungsi-Fungsi Tertentu di PT Pupuk Sriwidjaja Palembang;

6. Surat Keputusan Direksi PT Pupuk Sriwidjaja Palembang Nomor: SK/DIR/412/2022 tanggal 12 Desember 2022 tentang Struktur Organisasi PT Pupuk Sriwidjaja Palembang sebagaimana telah diubah beberapa kali dan terakhir diubah dengan Surat Keputusan Direksi PT Pupuk Sriwidjaja Palembang Nomor: SK/DIR/437/2023 tanggal 01 Desember 2023 tentang Penyempurnaan Struktur Organisasi di Lingkungan Kompartemen Administrasi Keuangan Direktorat Keuangan & Umum PT Pupuk Sriwidjaja Palembang;

M E M U T U S K A N

Menetapkan :

PERTAMA : Memberlakukan Pedoman Pengelolaan Keamanan Informasi PT Pupuk Sriwidjaja Palembang sebagaimana dimaksud dalam Lampiran Surat Keputusan Direksi ini.

KEDUA : Menginstruksikan kepada Senior Vice President Transformasi Bisnis, Vice President Mitra Bisnis dan Layanan TI PSP dan pimpinan unit kerja terkait lainnya untuk melaksanakan Surat Keputusan Direksi ini dengan sebaik-baiknya dan penuh tanggung jawab.

KETIGA : Setiap pejabat/karyawan Perusahaan yang terlibat dalam penerapan Surat Keputusan Direksi ini wajib memenuhi aspek kepatuhan dengan cara memastikan setiap tindakan yang dilakukan sesuai dengan Surat Keputusan Direksi ini dan ketentuan terkait lainnya serta bertanggungjawab sesuai dengan kewenangannya.

KEEMPAT : Setiap pejabat/karyawan Perusahaan yang terlibat dalam penerapan Surat Keputusan Direksi ini, sebagai *risk owner,* wajib mengelola risiko dengan cara mengidentifikasi, menganalisis, mengevaluasi dan melaporkan *progress* perlakuan risiko secara rutin, termasuk risiko *fraud* di proses bisnis masing-masing.

KELIMA : Bagi pejabat/karyawan Perusahaan yang lalai/berbuat kesalahan dalam melaksanakan Surat Keputusan Direksi ini yang berdampak kerugian bagi Perusahaan akan dikenakan sanksi sesuai ketentuan Perusahaan dan Perundang-undangan yang berlaku.

KEENAM : Surat Keputusan Direksi ini berlaku terhitung mulai tanggal ditetapkan.

PUSRI
PUPUK SRIWIDJAJA
PALEMBANG

PUPUK INDONESIA
HOLDING COMPANY

KETUJUH : Hal-hal lain yang belum cukup diatur dalam Surat Keputusan Direksi ini akan diatur dalam ketentuan tersendiri, dan apabila terdapat kekeliruan di dalamnya akan diadakan perubahan dan perbaikan sebagaimana mestinya.

Salinan Surat Keputusan ini disampaikan kepada:

1. Direksi (3x);
2. Seluruh SVP
3. VP Mitra Bisnis & Layanan TI PSP;

DISALIN SESUAI DENGAN ASLINYA OLEH
SVP TRANSFORMASI BISNIS

AGUS WALUYO
Badge No 00.0422

DITETAPKAN DI : PALEMBANG
PADA TANGGAL : 14 NOVEMBER 2023
Direksi,

d.t.o

DACONI KHOTOB
Direktur Utama

"S A L I N A N"
Lampiran
SK Direksi PT Pusri Palembang
Nomor : SK/DIR/430/2023
Tanggal : 14 November 2023

PEDOMAN
PENGELOLAAN KEAMANAN INFORMASI

Revisi	Tanggal	Alasan Revisi
0	14 Nov 2023	Penerbitan Pertama kali

DISTRIBUSI KE :

1. DIREKTUR UTAMA	8. SVP TEKNOLOGI	15. SVP SBU JPP
2. DIREKTUR OPERASI & PRODUKSI	9. SVP UMUM	16. SVP TRANSFORMASI BISNIS
3. DIREKTUR KEUANGAN & UMUM	10. SVP RENDAL PEMELIHARAAN	17. VP MITRA BISNIS & LAYANAN TI PSP
4. SVP SEKPER & TATA KELOLA	11. SVP RANTAI PASOK	
5. SVP SPI	12. SVP TEKNIK & PENGEMBANGAN	
6. SVP ADM KEUANGAN	13. SVP SDM	
7. SVP OPERASI	14. SVP SBU MANAJEMEN ASET	

DISUSUN OLEH	DIPERIKSA OLEH	DISETUJUI OLEH
d.t.o	d.t.o	d.t.o
AGUS WALUYO	*FILIUS YULIANDI*	*DACONI KHOTOB*
SVP TRANSFORMASI BISNIS	**DIREKTUR OPERASI & PRODUKSI**	**DIREKTUR UTAMA**
AVP PPSMT	*VP SMTI*	

DISALIN SESUAI DENGAN ASLINYA OLEH SVP TRANSFORMASI BISNIS

PUSRI
PUPUK SRIWIDJAJA PALEMBANG

AGUS WALUYO
Badge No. 00.0422

PUSRI PUPUK SRIWIDJAJA PALEMBANG

NO DOKUMEN : **PSP-TFB-PD-012**

DAFTAR ISI

DAFTAR ISI i
CATATAN PERUBAHAN DOKUMEN ii
1. TUJUAN 1
2. RUANG LINGKUP 1
3. REFERENSI 2
4. PRINSIP-PRINSIP 2
5. DEFINISI 4
6. KETENTUAN UMUM 6
7. PENGELOLAAN UMUM MANAJEMEN KEAMANAN TI 7
8. PENGELOLAAN KENDALI KEAMANAN ORGANISASI 7
9. PENGELOLAAN KENDALI KEAMANAN ORANG 21
10. PENGELOLAAN KENDALI KEAMANAN FISIK 23
11. PENGELOLAAN KENDALI KEAMANAN TEKNOLOGI 28
12. ALUR PROSES 39
13. LAMPIRAN 39

CATATAN PERUBAHAN DOKUMEN

No.	Bab/Sub Bab Halaman	Perincian Perubahan	Revisi Ke-	Tanggal
1.	Seluruh	Penerbitan Pertama	0	14 Nov 2023

1. TUJUAN

Pedoman Pengelolaan Keamanan Informasi ini menyatakan komitmen dan arahan dari Perusahaan untuk melaksanakan prinsip-prinsip keamanan informasi. Pedoman Pengelolaan Keamanan Informasi ini disusun dengan tujuan:

1.1. Melindungi kerahasiaan, keutuhan, dan ketersediaan sumber daya informasi Perusahaan dari segala bentuk gangguan dan ancaman baik dari dalam maupun luar, yang dilakukan secara sengaja atau tidak;

1.2. Mengoptimalkan pengelolaan risiko penggunaan Teknologi Informasi, dengan mencegah dan mengurangi dampak insiden keamanan sehingga dapat memelihara dan meningkatkan reputasi Perusahaan;

1.3. Mendorong manajemen dan seluruh Sumber Daya Manusia (SDM) Perusahaan untuk memiliki tingkat kesadaran (*awareness*), pengetahuan dan keterampilan yang memadai, serta bertanggung jawab dalam mengakses informasi milik Perusahaan agar dapat memenuhi kewajiban mereka dalam menjaga keamanan aset informasi;

1.4. Memiliki sumber daya yang memadai untuk melaksanakan program keamanan informasi yang efektif;

1.5. Memastikan kemampuan Dept. TI untuk melanjutkan aktifitasnya dalam hal terjadi insiden keamanan informasi yang signifikan atau ancaman terhadap sistem informasi Perusahaan;

1.6. Memastikan terpenuhinya kepatuhan terhadap undang-undang, peraturan dan ketentuan hukum lainnya yang berlaku bagi Perusahaan;

1.7. Memastikan konsistensi dalam menerapkan Sistem Manajemen Keamanan Informasi di lingkup Perusahaan.

2. RUANG LINGKUP

Pedoman ini memberikan panduan dalam pengelolaan pengamanan seluruh sumber daya informasi yang ada dan digunakan di Perusahaan dan unit terkait sebagai pengguna layanan Teknologi Informasi yang meliputi:

2.1. Organisasi dan Lokasi: meliputi seluruh unit kerja Perusahaan di seluruh Indonesia baik kantor pusat maupun kantor cabang dan lokasi mitra kerja,*vendor* serta pihak eksternal lainnya yang menyediakan dan / atau mendukung layanan Teknologi Informasi.

2.2. Informasi: Mencakup seluruh informasi yang dihasilkan atau diterima oleh Perusahaan yang harus dilindungi sesuai tingkat sensitivitas, kritikalitas ataupun kerahasiaannya yang disimpan dalam media apapun, baik dalam bentuk manual (kertas) maupun file elektronik atau didistribusikan dengan metode apapun;

2.3. Proses dan Layanan Teknologi Informasi: Pengelolaan dan penyediaan layanan. Teknologi

Informasi yang mencakup antara lain: Pengelolaan *Data Center* (DC), *Disaster Recovery Center* (DRC), *Network Operation Center, Service Desk* dan infrastruktur Teknologi Informasi lainnya;

2.4. Pengguna (*user*): meliputi seluruh pengguna informasi dan sistem informasi milik Perusahaan, baik pengguna internal maupun pengguna eksternal (mitra dan *vendor*) serta pihak eksternal lainnya yang melakukan akses terhadap informasi dan sistem informasi organisasi;

2.5. Pedoman ini merupakan bagian dari Pedoman Tata Kelola Teknologi Informasi yang secara khusus membahas komitmen dan kendali-kendali keamanan informasi yang menjadi komitmen perusahaan dalam rangka memenuhi persyaratan Standar ISO 27001 versi terkini dan peraturan perundangan yang berlaku.

3. REFERENSI

Pedoman Pengelolaan Keamanan Informasi Dept. TI ini mengacu pada peraturan dan dokumen berikut:

3.1 SNI ISO/IEC 27001:2022 Keamanan Informasi, Keamanan Siber, dan Proteksi Privasi - Sistem Manajemen Keamanan Informasi - Persyaratan;

3.2 Peraturan Menteri Badan Usaha Milik Negara Nomor PER-02/MBU/03/2023 Tentang Pedoman Tata Kelola dan Kegiatan Korporasi Signifikan Badan Usaha Milik Negara;

3.3 Pedoman Rencana SMKI PT Pupuk Sriwidjaja Palembang;

3.4 Daftar Undang-Undang, Peraturan, Kebijakan, Pedoman, Prosedur, Instruksi Kerja dan ketentuan hukum lainnya yang berlaku bagi Perusahaan serta Kewajiban-kewajiban Kontrak.

Selain itu, isi dari Pedoman ini juga diadopsi dari standar internasional ISO/IEC 27001:2022 yang meliputi 4 (empat) domain pengendalian keamanan informasi, dengan fokus pada persyaratan pengendalian keamanan. Cakupan dari domain pengendalian keamanan informasi antara lain adalah pada Kendali Organisasi, Kendali Orang, Kendali Fisik dan Kendali Teknologi.

Seluruh unit kerja dan SDM yang terkait dengan domain-domain keamanan informasi tersebut wajib melaksanakan pengendalian keamanan informasi sesuai dengan pedoman lebih terinci yang dapat disusun dengan mengacu pada pedoman ini dan prosedur formal yang terkait lainnya

4. PRINSIP-PRINSIP

4.1 Efisien

Bahwa Pedoman yang sudah disusun dapat meningkatkan kinerja pengelolaan keamanan informasi Perusahaan.

4.2 Efektif

Bahwa Pedoman yang sudah disusun harus dapat memberikan manfaat bagi Perusahaan dalam mencapai sasaran yang telah ditetapkan.

4.3 Akuntabel

Seluruh data dan informasi yang ada dalam Pedoman ini dapat dipertanggungjawabkan kebenarannya.

4.4 Berintegrasi

Dalam pelaksanaan pedoman ini harus memenuhi kaidah *Good Corporate Governance* (GCG), dilakukan secara profesional, independen, dan bebas dari benturan kepentingan serta dilaksanakan sesuai aturan dan ketentuan yang berlaku.

4.5 Kepastian Hukum

Pelaksanaan pedoman ini mengutamakan landasan peraturan perundang-undangan dan ketentuan internal yang berlaku, serta mempertimbangkan aspek kepatutan dan kewajaran, dan dapat memberikan perlindungan hukum bagi pihak terkait.

4.6 Integritas

Bahwa aset teknologi informasi sensitif dan kritikal milik Perusahaan hanya dapat diolah atau ditangani oleh pihak-pihak yang berhak dan memang dimaksudkan untuk mengolah atau menangani informasi tersebut. dan tidak dimodifikasi, dihapus, atau dirusak oleh pihak yang tidak berwenang.

4.7 Ketersediaan

Bahwa aset teknologi informasi sensitif dan kritikal milik Perusahaan tersedia serta dapat digunakan oleh pihak yang berwenang dalam semua kondisi, terutama saat dibutuhkan, dan aman dari kemungkinan serangan yang dapat menyebabkan kehilangan atau ketidakbergunaan informasi.

4.8 Kerahasiaan

Bahwa aset teknologi informasi sensitif dan kritikal milik Perusahaan hanya dapat diakses oleh pihak-pihak yang memang memiliki otorisasi untuk mengakses informasi tersebut.

4.9 Kehati-hatian

Dalam proses implementasi pedoman ini harus berdasarkan pada asas kehati-hatian, yakni dengan memperhitungkan dampak/risiko yang terkecil bagi Perusahaan dan/atau Pejabat/Personil terkait.

4.10 Manajemen Risiko

Perusahaan melakukan analisa dan penilaian risiko keamanan informasi atas pemangku kepentingan serta isu-isu eksternal dan internal yang berpengaruh pada keamanan informasi.

4.11 Komunikasi

Perusahaan mengkomunikasikan Pedoman ini kepada pemangku kepentingan secara teratur dalam jangka waktu berkala.

4.12 Pemantauan dan Evaluasi

Dalam rangka meningkatkan efektivitas penerapan SMKI, Perusahaan secara berkala melakukan pemantauan atas kinerja dan melakukan perbaikan serta penyempurnaan jika dalam proses pemantauan tersebut terdapat ketidaksesuaian.

5. DEFINISI

5.1. Aset Informasi adalah segala bentuk informasi yang berharga dan memiliki nilai bagi PT Pupuk Sriwidjaja Palembang. Aset Teknologi Informasi dapat berupa *Database* (kumpulan data pendukung proses bisnis yang tersimpan di dalam sistem TI), *Software*/ perangkat lunak (aplikasi, *system software*, ERP, *software* pembantu pengembangan sistem, sistem operasi, dan alat bantu pendukung kerja), Aset Fisik (perangkat komputer, media penyimpanan data).

5.2. *Baseline Security Configuration* adalah konfigurasi suatu sistem yang disusun untuk memaksimalkan pengamanan melalui penentuan sejumlah parameter teknis yang ada, yang penerapannya harus dilakukan sebelum sistem tersebut digunakan secara operasional dimana penetapannya dapat menggunakan referensi yang diterbitkan oleh pabrikan teknologi tersebut atau oleh organisasi yang secara khusus mengeluarkan standar untuk kepentingan publik.

5.3. Dept. TI adalah Departemen Mitra Bisnis Layanan Teknologi Informasi (MBL TI) Perusahaan, yang bertanggung jawab ataupun dikuasakan untuk mengelola aset, SDM, anggaran, maupun tata kelola TI di Perusahaan.

5.4. Evaluasi Risiko adalah proses yang membandingkan estimasi besaran suatu risiko dengan kriteria yang sudah terdefinisi untuk menetapkan tingkatan risiko.

5.5. Hak Akses adalah kewenangan menggunakan suatu sumber daya informasi yang jenis dan tingkatannya disesuaikan dengan kebutuhan kerja pengguna dan disetujui oleh Pemilik Aset Informasi atau pimpinan unit kerja yang bersangkutan.

5.6. Insiden Keamanan Informasi adalah kejadian yang tidak diinginkan dan yang melanggar pedoman atau prosedur dalam pengelolaan keamanan informasi sehingga menimbulkan ancaman terhadap kondisi keamanan sumber daya informasi atau mengakibatkan gangguan terhadap proses kerja organisasi.

5.7. Kajian Risiko adalah keseluruhan proses identifikasi, pengkajian, pengukuran, analisa, pemantauan, dan evaluasi risiko.

5.8. Keamanan Informasi adalah pemeliharaan dan perlindungan terhadap kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) informasi termasuk otentikasi, *accountability*, *non-repudiation* dan *reliability*.

5.9. Kerahasiaan adalah karakteristik informasi yang hanya dapat diketahui oleh mereka yang berwenang melalui cara yang diizinkan.

5.10. Ketersediaan adalah karakteristik informasi yang menjamin bahwa pengguna yang berwenang dapat mengakses informasi pada saat diperlukan.

5.11. Keutuhan adalah karakteristik informasi yang menjamin informasi akurat, lengkap, tidak berubah selama pengiriman dan pengolahannya.

5.12. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai,

makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca dengan disajikan dalam berbagai kemasan dan format secara elektronik ataupun nonelektronik yang dihasilkan, disimpan, dikelola, dikirim, dan/atau diterima oleh suatu organisasi.

5.13. Koordinator Keamanan Teknologi Informasi adalah VP Dept. TI yang bertugas mengidentifikasi dan mengatasi masalah layanan Teknologi Informasi atau insiden keamanan informasi yang diketahuinya dan/atau dilaporkan kepadanya.

5.14. Kustodi adalah kendali atau tanggung jawab terhadap aset berharga yang harus disimpan dan dijaga dengan penuh kewaspadaan dan dengan keamanan tingkat tinggi.

5.15. Layanan Teknologi Informasi (Layanan TI) adalah fasilitas yang terdiri dari gabungan komponen teknologi, proses, dan personil dalam rangka penyelenggaraan sistem informasi yang direncanakan, dikembangkan, dioperasikan, dan dipelihara oleh Dept. TI baik secara terpusat maupun terdistribusi, yang digunakan untuk memenuhi kepentingan pemenuhan tugas pokok dan fungsi unit kerja terkait maupun Perusahaan pada umumnya.

5.16. Manajemen Representatif adalah SVP Transformasi Bisnis yang ditetapkan minimum oleh Direktur Utama.

5.17. *Mobile Computing* adalah penggunaan perangkat komputasi jinjing (*portable*) seperti *notebook*, *tablet* dan *mobile device* untuk melakukan akses, pengolahan data dan penyimpanannya.

5.18. Pemilik Sumber Daya Teknologi Informasi (TI) adalah pihak yang ditetapkan sebagai penanggung jawab terhadap pengamanan sumber daya Teknologi Informasi atau proses kerja di Perusahaan atau pimpinan unit kerja pemilik data atau informasi.

5.19. Perangkat Lunak adalah suatu paket aplikasi yang memungkinkan pengguna untuk melakukan tugas-tugas tertentu yang bertujuan untuk meningkatkan efektivitas dan efisiensi kerja. Selanjutnya Perangkat lunak disebut sebagai Aplikasi.

5.20. Perangkat Lunak Open-Source adalah perangkat lunak untuk komputer yang beserta kode program disediakan oleh pemilik hak cipta (*copyright holder*) untuk dipelajari, diubah, dan disebarkan ke siapa saja dan digunakan untuk kepentingan apapun.

5.21. Perusahaan dengan huruf P besar adalah PT Pupuk Sriwidjaja Palembang.

5.22. Pihak Eksternal adalah pihak luar yang melaksanakan kerjasama dengan Perusahaan atas dasar perjanjian atau kontrak yang disepakati bersama. Pihak eksternal meliputi *vendor*, kontraktor, mitra dan tamu.

5.23. *Recovery Point Objective* (RPO) adalah titik waktu saat data dipulihkan setelah terjadi suatu gangguan disrupsi.

5.24. *Recovery Time Objective* (RTO) adalah jangka waktu saat level minimum layanan dan/atau produk serta sistem, aplikasi, atau fungsi pendukung dipulihkan setelah terjadi suatu gangguan disrupsi.

5.25. *Service Desk* adalah fungsi Unit Kerja TI Perusahaan yang berperan sebagai *contact person* Dept.

TI dalam rangkaian proses layanan TI serta pemecahan masalah dan perbaikannya yang terkait dengan operasional TI.

5.26. Sumber Daya Manusia Teknologi Informasi (SDM TI) adalah manusia yang dipekerjakan pada suatu organisasi sebagai perencana, pelaksana, dan penggerak untuk mencapai tujuan organisasi.

5.27. Sumber Daya Teknologi Informasi (TI) adalah SDM TI serta data, informasi, sistem informasi, aplikasi/*software*, infrastruktur/*hardware* suatu sistem TI.

5.28. Teknologi Informasi (TI) adalah istilah umum untuk teknologi yang membantu manusia dalam membuat, mengubah, menyimpan, mengomunikasikan, dan/atau menyebarkan informasi. Teknologi informasi meliputi: *Software* (*Database*, *Desktop* & *Collaboration*, *Application*, *Operating System* & *Virtualization*); *Hardware* (*End User Computing*, *Networking*, *Data Center*, *Server* & *Storage Infrastructure*); *Information Management* (*Dashboard* & *Portal*, *Business Intelligence*/ *Executive Information System*, *Knowledge Management*, *Data Warehouse*); *Communications* (*Data*, *Voice*, *Converge*); dan *Services* & *Consulting* (*Service Desk*, *Support* & *Development*).

5.29. Teleworking adalah pengaturan kerja yang fleksibel dimana pegawai diizinkan untuk bekerja dan mengakses sistem informasi perusahaan dari luar lingkungan kantor perusahaan, misalnya dari rumah atau lokasi tertentu lainnya yang ditetapkan.

5.30. Sistem Manajemen Keamanan Informasi (SMKI) adalah Sistem Manajemen Keamanan Informasi yang sesuai dengan persyaratan standar SNI ISO/IEC 27001 versi terkini.

5.31. VP Dept. TI adalah pimpinan unit kerja Departemen MBL TI PSP.

6. KETENTUAN UMUM

6.1 Aspek Kepatuhan

Setiap Pejabat/Karyawan Perusahaan yang terlibat dalam penerapan Pedoman ini wajib memenuhi aspek kepatuhan dengan cara memastikan setiap tindakan yang dilakukan sesuai dengan Pedoman ini dan bertanggungjawab sesuai dengan kewenangannya.

Bagi Pejabat/Karyawan Perusahaan yang lalai/berbuat kesalahan dalam melaksanakan Pedoman ini yang mengakibatkan kerugian bagi Perusahaan, dikenakan sanksi sesuai dengan ketentuan Perusahaan dan peraturan perundang-undangan yang berlaku.

6.2 Aspek Pengelolaan Risiko

Setiap Pejabat/Karyawan Perusahaan yang terlibat dalam penerapan Pedoman ini, sebagai *risk owner*, wajib mengelola risiko dengan cara mengidentifikasi, menganalisis, mengevaluasi, dan melaporkan kemajuan (*progress*) perlakuan risiko secara rutin, termasuk risiko *fraud* pada proses bisnis masing-masing.

7. PENGELOLAAN UMUM MANAJEMEN KEAMANAN TI

7.1 Perusahaan menetapkan kerangka kerja keamanan TI yang bertujuan untuk menjamin aspek-aspek sebagai berikut:

7.1.1 Kerahasiaan (*confidentiality*), yaitu bahwa informasi dan layanan TI perusahaan harus dilindungi dari akses oleh pihak yang tidak berwenang;

7.1.2 Integritas (*integrity*), yaitu bahwa informasi dan layanan TI perusahaan harus terjamin kelengkapan dan akurasinya serta terhindar dari perubahan secara tidak sah;

7.1.3 Ketersediaan (*availability*), yaitu bahwa informasi dan layanan TI perusahaan harus tersedia untuk diakses dan/atau digunakan pada saat diperlukan oleh pihak-pihak yang berwenang/berkepentingan.

7.2 Demi menjamin efektivitas dan efisiensi Sistem Manajemen Keamanan Informasi (SMKI) Perusahaan, seluruh pegawai Perusahaan secara bersama-sama memberikan komitmen terhadap pelaksanaan SMKI melalui:

7.2.1 Penerapan Pedoman dan pencapaian sasaran keamanan informasi;

7.2.2 Pengelolaan ketersediaan dari sumber daya yang dibutuhkan dalam rangka implementasi SMKI;

7.2.3 Menjalankan tugas dan tanggung jawab yang ditentukan terkait pengelolaan keamanan informasi;

7.2.4 Memastikan koordinasi implementasi terhadap kendali keamanan informasi telah dilakukan secara berkala;

7.2.5 Peningkatan yang berkesinambungan yang dijabarkan dalam program SMKI.

8. PENGELOLAAN KENDALI KEAMANAN ORGANISASI

8.1 Pemisahan (segregasi) Tugas.

Perusahaan harus menjamin dilakukannya pemisahan tugas SDM pada proses-proses yang berbasis komputer yang melibatkan informasi rahasia, berharga dan rawan, agar tidak ada SDM yang memiliki kendali menyeluruh terhadap sumber daya informasi penting.

8.2 *Threat Intelligence* / Pengetahuan terhadap Ancaman.

Informasi tentang ancaman yang ada atau yang muncul dikumpulkan dan dianalisis untuk:

8.2.1 Memfasilitasi tindakan terinformasi untuk mencegah ancaman yang membahayakan bagi organisasi.

8.2.2 Mengurangi dampak ancaman tersebut.

8.3 Keamanan Informasi dalam Manajemen Proyek TI.

8.3.1 Keamanan informasi akan diintegrasikan ke dalam manajemen proyek TI untuk

memastikan risiko keamanan informasi ditangani sebagai bagian dari manajemen proyek.

8.3.2 Risiko keamanan informasi dinilai dan ditangani pada tahap awal dan secara periodik, sebagai bagian dari pengendalian risiko proyek sepanjang siklus hidup proyek.

8.3.3 Persyaratan keamanan informasi ditangani pada tahap awal proyek.

8.3.4 Dept. TI menetapkan dan mendokumentasikan secara jelas persyaratan-persyaratan keamanan informasi yang relevan sebelum melakukan proyek pembangunan, perluasan, atau pengadaan sistem informasi baru.

8.3.5 Risiko keamanan informasi yang terkait dengan pelaksanaan proyek, seperti keamanan aspek komunikasi internal dan eksternal dipertimbangkan dan ditangani sepanjang siklus hidup proyek.

8.3.6 Progres penanganan risiko keamanan informasi akan dipantau, sedangkan efektivitas penanganan akan dievaluasi dan diuji.

8.4 Inventori informasi dan aset terkait lainnya.

8.4.1 Perusahaan harus memiliki daftar inventaris Sumber Daya TI yang berisikan seluruh Sumber Daya TI utama, seperti perangkat lunak, perangkat keras dan layanan yang akan dilindungi. Daftar Inventaris harus secara jelas mengidentifikasi setiap sumber daya, pemilik sumber daya, dan lokasinya. Pengelolaan dan pengkinian daftar inventaris Sumber Daya TI ini dilakukan oleh Dept. TI.

8.4.2 Pemilik Sumber Daya TI bertanggung jawab atas perlindungan keamanan seluruh Sumber Daya TI yang berada di bawah pengawasannya.

8.4.3 Perusahaan menetapkan Pedoman dan aturan penggunaan Sumber Daya TI bagi SDM dan Pihak Eksternal yang ditetapkan oleh Pejabat Otorisator terkait. Seluruh pengguna Sumber Daya TI tanpa terkecuali, wajib mematuhi ketentuan dan aturan yang telah ditetapkan, serta harus melaporkan kepada Dept. TI bila melihat terjadinya pelanggaran terhadap Pedoman ini.

8.5 Penggunaan Informasi dan aset terkait lainnya yang diperbolehkan.

8.5.1 Penggunaan Sumber Daya TI harus dimanfaatkan sebesar-besarnya untuk kepentingan dan kegiatan yang menunjang usaha organisasi Perusahaan.

8.5.2 Dept. TI berhak mematikan proses penggunaan sumber daya Teknologi Informasi atau menutup hak akses pengguna yang berpotensi mengganggu kinerja sistem informasi atau dalam rangka memelihara kinerja sistem TI Perusahaan.

8.6 Pengembalian Aset dan Informasi.

8.6.1 Seluruh pegawai yang berhenti bekerja atau mutasi harus mengembalikan seluruh aset dan informasi yang dipergunakan selama bekerja sesuai dengan ketentuan yang berlaku.

8.6.2 Pihak ketiga yang habis masa kontrak kerjanya harus mengembalikan seluruh aset dan

informasi yang dipergunakan selama bekerja di Perusahaan.

8.7 Klasifikasi dan Pelabelan Aset dan Informasi.

8.7.1 Klasifikasi Sumber Daya TI utama merujuk pada Pedoman Pengelolaan Aset.

8.7.2 Penanganan setiap Sumber Daya TI harus sesuai dengan kritikalitas dan tingkat risiko yang ada.

8.8 Transfer/Pemindahan Aset dan Informasi.

8.8.1 Transfer/pemindahan informasi dan perangkat lunak antara Perusahaan dengan pihak eksternal hanya akan dilakukan atas persetujuan tertulis kedua belah pihak. Khusus transfer/pemindahan informasi digital harus disetujui oleh VP Dept. TI Perusahaan.

8.8.2 Dept. TI Perusahaan harus menjamin bahwa pertukaran informasi penting dan rawan hanya dilakukan setelah melalui suatu pengkajian risiko yang memadai dan setelah dilakukan penetapan ketentuan-ketentuan keamanan informasi dalam perjanjian pertukaran informasi antara pihak yang terkait.

8.8.3 Dept. TI Perusahaan harus menerapkan pengendalian keamanan informasi untuk pengiriman informasi melalui surat elektronik dalam rangka menghindari akses pihak yang tidak berwenang

8.8.4 Aset informasi yang dikirim dengan menggunakan jasa layanan pengiriman kurir atau pos rawan diakses oleh pihak yang tidak berwenang selama pengiriman. Oleh karena itu, Perusahaan menerapkan kendali-kendali sebagai berikut:

a. Mencatat secara lengkap dan jelas identitas kurir yang digunakan.
b. Mengemas sumber daya informasi dalam kemasan yang baik dan kuat yang mampu melindungi kandungannya dari kerusakan fisik selama pengiriman.

8.8.5 SDM harus menghindari pembicaraan menyangkut informasi penting Perusahaan bila sedang berada atau berkomunikasi di tempat umum.

8.8.6 Informasi internal Dept. TI Perusahaan yang disediakan bagi masyarakat umum harus disetujui oleh pemilik aset informasi dan harus dilindungi keutuhannya dari modifikasi oleh pihak yang tidak berwenang.

8.9 Kendali dan Hak Akses.

8.9.1 Hak penggunaan/akses terhadap aset-aset informasi harus diberikan sesuai dengan kebutuhan fungsi dan tugas SDM dan diberikan berdasarkan prinsip minimum/seperlunya yaitu cukup untuk memenuhi kebutuhan dalam menjalankan tugasnya.

8.9.2 Setiap permintaan hak penggunaan/akses oleh SDM harus disetujui oleh atasan dari SDM yang bersangkutan minimal setingkat VP Unit Kerja terkait.

8.9.3 Hak akses khusus, yakni hak untuk menggunakan aset informasi yang penting / rawan seperti sistem operasi, *storage devices*, *file server*, dan aplikasi-aplikasi yang penting /

rawan hanya boleh diberikan kepada user yang terlatih.

8.9.4 Hak akses khusus hanya boleh digunakan untuk melakukan pekerjaan yang hanya bisa dilaksanakan melalui akun (*account*) akses khusus.

8.9.5 Pemberian hak akses khusus TI harus dengan persetujuan penugasan dari VP Dept TI.

8.9.6 Pemakaian hak akses akan dipantau dan dievaluasi secara berkala untuk menjamin kesesuaian pemakaiannya.

8.9.7 Hasil evaluasi akan dibahas dan dianalisa oleh Koordinator Keamanan TI dan ditindaklanjuti oleh pihak yang terkait.

8.10 Pengelolaan Identitas.

8.10.1 Identitas spesifik yang diberikan kepada seseorang hanya akan terkait dengan satu orang tersebut, agar akuntabel atas tindakan yang dilakukan.

8.10.2 Sedangkan identitas yang diberikan kepada beberapa orang (misalnya berbagi identitas) hanya diizinkan jika diperlukan untuk alasan bisnis atau operasional serta tunduk pada persetujuan dan dokumentasi khusus.

8.10.3 Identitas harus dinonaktifkan secepatnya jika tidak lagi dibutuhkan (misalnya dalam hal entitas terkait telah dihapus atau tidak lagi digunakan, atau jika SDM telah berpindah tugas atau mengundurkan diri).

8.10.4 Semua catatan mengenai penggunaan dan manajemen identitas akan dikelola dan disimpan dengan baik.

8.11 Informasi Autentikasi.

8.11.1 Pengguna (user) harus memakai *password* yang tidak mudah ditebak oleh orang lain.

8.11.2 *Password* awal yang diberikan oleh administrator sistem/aplikasi hanya bisa digunakan sekali saja dan selanjutnya harus diganti sebelum pengguna dapat memakai lebih lanjut hak aksesnya pada sistem/aplikasi terkait.

8.11.3 *Password* terdiri dari kombinasi huruf, angka dan karakter khusus / simbol dengan panjang minimal sebanyak 8 karakter, serta tidak menggunakan password yang sudah pernah digunakan sebelumnya.

8.11.4 *Password* harus dijaga kerahasiaannya dan harus diperlakukan sebagai berikut:

a. Tidak boleh dipakai bersama (*shared*) dengan orang lain.
b. Tidak boleh diberitahukan kepada orang lain.
c. Tidak boleh dituliskan (*hard coded*) dalam bentuk apapun.
d. Tidak boleh ditulis pada media yang diletakkan di tempat yang mudah terlihat orang lain.

8.11.5 *Password* seluruh pengguna sistem informasi yang menyimpan atau mengelola data rahasia harus diganti secara periodik tertentu sesuai ketentuan Perusahaan atau segera diganti bila telah diketahui orang lain atau jika diperintahkan oleh Dept. TI Perusahaan.

8.11.6 Bila terjadi kegagalan *log on* secara berturut-turut maka akun pengguna (*user account*) tidak dapat dipakai dan pengguna harus menghubungi *Service Desk* untuk memfungsikannya kembali. Parameter kegagalan *log on* secara berurutan tergantung pada pengaturan dari masing-masing aplikasi..

8.11.7 Pemakaian *User ID* dan kegiatan yang dilakukan, akan dicatat dan direkam untuk tujuan pemantauan dan tindakan terkait.

8.12 Keamanan Informasi dalam Hubungan Pemasok (*Supplier Relationship*).

Terkait dengan Hubungan Pemasok, Perusahaan akan:

8.12.1 Melakukan identifikasi dan dokumentasi jenis pemasok terkait kerahasiaan, keutuhan, dan ketersediaan informasi organisasi.

8.12.2 Menetapkan cara menilai dan memilih pemasok sesuai dengan sensitivitas informasi, produk dan layanan yang diberikan oleh pemasok.

8.12.3 Menilai dan memilih produk atau layanan pemasok yang memiliki kendali keamanan informasi yang cukup dan melakukan peninjauan; khususnya akurasi dan kelengkapan kendali yang diimplementasikan oleh pemasok yang memastikan keutuhan informasi dan pemrosesan informasi pemasok serta keamanan informasi organisasi.

8.12.4 Mendefinisikan informasi organisasi, layanan TI dan infrastruktur fisik yang dapat diakses, dipantau, dikendalikan atau digunakan oleh pemasok.

8.12.5 Mendefinisikan jenis komponen dan layanan infrastruktur TI yang disediakan oleh pemasok yang memiliki dampak pada kerahasiaan, keutuhan dan ketersediaan informasi organisasi.

8.12.6 Menilai dan mengelola risiko keamanan informasi yang terkait dengan:

a. Penggunaan informasi organisasi dan aset terkait lainnya oleh pemasok, termasuk risiko yang berasal dari personil pemasok yang berpotensi berbahaya.
b. Kerusakan atau kerentanan produk (termasuk komponen dan subkomponen perangkat lunak yang digunakan dalam produk ini) atau layanan yang disediakan oleh pemasok.

8.12.7 Memantau kepatuhan terhadap persyaratan keamanan informasi yang ditetapkan untuk setiap jenis pemasok dan setiap jenis akses, termasuk tinjauan dari Pihak Ketiga dan validasi produk.

8.12.8 Melakukan mitigasi ketidakpatuhan pemasok, baik terdeteksi melalui kegiatan pemantauan atau dengan cara lain.

8.12.9 Menangani insiden dan kontingensi yang terkait dengan produk dan layanan pemasok, termasuk tanggung jawab organisasi dan pemasok.

8.12.10 Jika diperlukan, dapat melakukan langkah-langkah pemulihan dan tindakan darurat untuk memastikan ketersediaan dari informasi dan pemrosesan informasi pemasok.

8.12.11 Memberikan *awareness* dan pelatihan bagi personil organisasi yang berinteraksi dengan

personil pemasok mengenai aturan keterlibatan yang tepat, kebijakan/pedoman spesifik, proses dan prosedur serta perilaku berdasarkan jenis pemasok dan level akses pemasok ke sistem dan informasi organisasi.

8.12.12 Mengelola transfer informasi yang diperlukan, aset terkait lainnya dan hal-hal yang perlu diubah, serta memastikan bahwa keamanan informasi terpelihara selama periode transfer.

8.12.13 Menentukan persyaratan pengakhiran hubungan pemasok yang aman, meliputi:

a. Pencabutan Hak Akses.
b. Penanganan informasi.
c. Penentuan kepemilikan atas hak kekayaan intelektual yang dikembangkan selama kerjasama.
d. Portabilitas informasi dalam hal perubahan pemasok atau pengerjaan internal.
e. Pengelolaan rekaman.
f. Pengembalian aset.
g. Penghapusan informasi dan aset terkait lainnya dengan aman.
h. Persyaratan kerahasiaan berkelanjutan.

8.12.14 Menentukan tingkat keamanan personil dan keamanan fisik yang diharapkan dari personil dan fasilitas pemasok.

8.13 Menangani Keamanan Informasi dalam Perjanjian dengan Pemasok.

8.13.1 Perjanjian dengan pemasok akan memuat hal-hal sebagai berikut:

a. Deskripsi informasi yang akan diberikan atau diakses dan metode pemberian atau akses informasi.
b. Persyaratan legal, statutori, regulatori, dan kontraktual, termasuk proteksi data, penanganan *Personally Identifiable Information* (PII), hak kekayaan intelektual, serta hak cipta dan deskripsi tentang bagaimana memastikan persyaratan tersebut terpenuhi.
c. Kewajiban setiap pihak dalam kontrak untuk mengimplementasikan serangkaian perangkat kendali yang disepakati, termasuk kendali akses, peninjauan kinerja, pemantauan, pelaporan dan audit, serta kewajiban pemasok untuk mematuhi persyaratan keamanan informasi organisasi.
d. Aturan penggunaan yang dapat diterima terhadap informasi dan aset terkait lainnya, termasuk penggunaan yang tidak dapat diterima jika diperlukan.
e. Prosedur atau ketentuan untuk otorisasi dan pemindahan otorisasi untuk penggunaan informasi organisasi dan aset terkait lainnya oleh personil pemasok.
f. Persyaratan keamanan informasi mengenai infrastruktur teknologi informasi pemasok; khususnya, persyaratan keamanan informasi minimum untuk setiap jenis informasi dan jenis akses untuk menjadi dasar setiap perjanjian pemasok individual berdasarkan

kebutuhan bisnis dan kriteria risiko organisasi.

g. Ganti rugi dan perbaikan atas kegagalan kontraktor untuk memenuhi persyaratan.
h. Persyaratan dan prosedur manajemen insiden (terutama notifikasi dan kolaborasi selama perbaikan insiden).
i. Persyaratan pelatihan dan *awareness* untuk prosedur dan persyaratan keamanan informasi spesifik (misalnya untuk respon insiden, prosedur otorisasi).
j. Ketentuan sub kontrak yang relevan, termasuk kendali yang perlu diimplementasikan seperti perjanjian tentang penggunaan sub pemasok (misalnya mempersyaratkan subpemasok mematuhi kewajiban yang sama dengan pemasok, mempersyaratkan pemasok memiliki daftar sub pemasok dan notifikasi sebelum perubahan).
k. Kontak yang relevan, termasuk narahubung untuk masalah keamanan informasi.
l. Persyaratan skrining - jika diizinkan secara legal - untuk personil pemasok, termasuk tanggung jawab untuk melakukan skrining dan prosedur notifikasi jika skrining belum selesai atau jika hasilnya menimbulkan keraguan atau kekhawatiran.
m. Mekanisme bukti dan keyakinan pembuktian pihak ketiga untuk persyaratan keamanan informasi yang relevan terkait dengan proses pemasok dan laporan independen tentang efektivitas kendali.
n. Hak untuk mengaudit proses dan kendali pemasok yang terkait dengan perjanjian.
o. Kewajiban pemasok untuk secara berkala menyampaikan laporan tentang efektivitas kendali dan perjanjian tentang perbaikan tepat waktu atas masalah yang diangkat dalam laporan.
p. Penyelesaian kerusakan dan proses penyelesaian konflik.
q. Menyediakan cadangan yang selaras dengan kebutuhan organisasi (dalam hal frekuensi dan jenis serta lokasi penyimpanan).
r. Memastikan ketersediaan fasilitas alternatif (yaitu lokasi pemulihan bencana) tidak rentan terhadap ancaman yang sama dengan fasilitas utama dan pertimbangan untuk kendali *fall back* (kendali alternatif) jika kendali utama gagal.
s. Memiliki proses manajemen perubahan yang memastikan notifikasi awal kepada organisasi dan kemungkinan organisasi tidak menerima perubahan.
t. Kendali keamanan fisik yang sesuai dengan klasifikasi informasi.
u. Kendali transfer informasi untuk memproteksi informasi selama transfer fisik atau logikal.
v. Pasal terminasi setelah berakhirnya perjanjian termasuk manajemen arsip, pengembalian aset, penghapusan informasi dan aset terkait lainnya secara aman dan kewajiban kerahasiaan yang sedang berlangsung.
w. Penyediaan metode penghancuran secara aman terhadap informasi organisasi yang

disimpan oleh pemasok segera setelah tidak lagi diperlukan.

x. Memastikan tersedianya dukungan serah terima kepada pemasok lain atau kepada organisasi itu sendiri, pada akhir kontrak.

8.14 Pengelolaan keamanan informasi dalam Rantai Pasokan (*supply chain*) TI.

Keamanan Rantai Pasokan TI akan mempertimbangkan hal-hal berikut ini:

8.14.1 Mendefinisikan persyaratan keamanan informasi untuk diterapkan pada akuisisi produk atau layanan TI.

8.14.2 Mensyaratkan bahwa pemasok layanan TI menginformasikan persyaratan keamanan organisasi di seluruh rantai pasokan jika mereka melakukan subkontrak untuk bagian dari layanan Teknologi informasi yang diberikan kepada organisasi.

8.14.3 Mensyaratkan bahwa pemasok produk TI menyebarluaskan praktik keamanan yang sesuai di seluruh rantai pasokan jika produk-produk tersebut mencakup komponen yang dibeli atau diperoleh dari pemasok lain atau entitas lain (misalnya subkontrak *Developer* perangkat lunak dan penyedia komponen perangkat keras).

8.14.4 Meminta pemasok produk TI memberikan informasi yang menjelaskan komponen perangkat lunak yang digunakan dalam produk.

8.14.5 Meminta pemasok produk TI memberikan informasi yang menjelaskan fungsi keamanan yang diimplementasikan dari produk mereka dan konfigurasi yang diperlukan untuk operasional yang aman.

8.14.6 Implementasi proses pemantauan dan metode yang dapat diterima untuk memvalidasi bahwa produk dan layanan TI yang dikirimkan sesuai dengan persyaratan keamanan yang dijanjikan.

8.14.7 Implementasi proses untuk mengidentifikasi dan mendokumentasikan komponen produk atau layanan yang sangat penting untuk memelihara fungsionalitas sehingga memerlukan peningkatan perhatian, pengawasan, dan tindak lanjut yang diperlukan ketika dibangun di luar organisasi terutama jika pemasok mengalihdayakan aspek produk atau komponen layanan kepada pemasok lain.

8.14.8 Mendapatkan keyakinan bahwa komponen kritikal dan asalnya dapat ditelusuri di seluruh rantai pasokan.

8.14.9 Mendapatkan keyakinan bahwa produk TI yang dikirimkan berfungsi sesuai harapan tanpa fitur yang tidak terduga atau tidak diinginkan.

8.14.10 Mengimplementasikan proses untuk memastikan bahwa komponen dari pemasok asli dan tidak diubah dari spesifikasinya.

8.14.11 Mendapatkan keyakinan bahwa produk TI mencapai level keamanan yang dipersyaratkan, misalnya melalui *common criteria recognition arrangement*.

8.14.12 Sertifikasi formal atau skema evaluasi seperti mendefinisikan aturan untuk berbagi informasi mengenai rantai pasokan dan potensi masalah dan pembobolan di antara organisasi dan pemasok.

8.14.13 Mengimplementasikan proses spesifik untuk mengelola siklus hidup komponen TI dan ketersediaan (*availability*) serta risiko keamanan terkait, termasuk mengelola risiko komponen yang tidak lagi tersedia karena pemasok tidak lagi beroperasi atau pemasok tidak lagi menyediakan komponen ini karena kemajuan teknologi.

8.15 Pemantauan, Peninjauan dan Pengelolaan Perubahan Layanan Pemasok.

Kendali ini akan melibatkan proses pengelolaan hubungan antara organisasi dengan pemasok dalam hal:

8.15.1 Memantau level kinerja layanan untuk memverifikasi kepatuhan terhadap perjanjian kontrak.

8.15.2 Memantau perubahan yang dilakukan oleh pemasok termasuk:

a. Peningkatan layanan yang ditawarkan saat ini.
b. Pengembangan aplikasi dan sistem baru.
c. Perhitungan kaji ulang tingkat risiko, termasuk tingkat kerawanan sistem dan proses terkait.
d. Kendali baru atau yang diubah untuk menyelesaikan insiden keamanan informasi dan untuk meningkatkan keamanan informasi.

8.15.3 Memantau perubahan dalam layanan pemasok termasuk:

a. Perubahan dan peningkatan jaringan.
b. Penggunaan teknologi baru.
c. Adopsi produk baru atau versi atau keluaran yang lebih mutakhir.
d. Alat dan lingkungan pengembangan baru.
e. Perubahan fisik lokasi fasilitas pelayanan.
f. Pergantian sub pemasok.
g. Sub kontrak dengan pemasok lain.

8.15.4 Meninjau laporan layanan yang dihasilkan oleh pemasok dan mengatur rapat kemajuan rutin sebagaimana ditentukan dalam perjanjian.

8.15.5 Melakukan audit terhadap pemasok dan subpemasok, sehubungan dengan tinjauan laporan auditor independen - jika tersedia - dan tindak lanjut atas masalah yang diidentifikasi.

8.15.6 Menyediakan informasi tentang insiden keamanan informasi dan meninjau informasi ini sebagaimana ditentukan dalam perjanjian dan pedoman serta prosedur pendukung apa pun.

8.15.7 Meninjau jejak audit pemasok dan rekaman peristiwa keamanan informasi, problem operasional, kegagalan, pelacakan kesalahan dan disrupsi yang terkait dengan layanan yang disediakan.

8.15.8 Merespon dan mengelola peristiwa atau insiden keamanan informasi yang teridentifikasi.

8.15.9 Mengidentifikasi dan mengelola kerentanan keamanan informasi.

8.15.10 Meninjau aspek keamanan informasi dari hubungan pemasok dengan pemasoknya sendiri.

8.15.11 Memastikan bahwa pemasok memelihara kapabilitas layanan yang cukup - bersama dengan rencana yang dapat diterapkan - yang dirancang untuk memastikan bahwa level keberlangsungan layanan yang disepakati dapat dipertahankan setelah kegagalan layanan atau bencana besar.

8.15.12 Memastikan bahwa pemasok bertanggung jawab untuk meninjau kepatuhan dan menegakkan persyaratan perjanjian.

8.15.13 Mengevaluasi secara reguler bahwa pemasok memelihara level keamanan informasi yang cukup.

8.16 Keamanan informasi untuk penggunaan layanan *cloud*.

Dept. TI mendefinisikan:.

8.16.1 Semua persyaratan keamanan informasi yang relevan terkait dengan penggunaan layanan *cloud*.

8.16.2 Kriteria pemilihan layanan *cloud* dan ruang lingkup penggunaan layanan *cloud*.

8.16.3 Peran dan tanggung jawab yang terkait dengan penggunaan dan manajemen layanan *cloud*.

8.16.4 Pembagian kendali keamanan informasi mana yang dikelola oleh Dept. TI dan mana yang dikelola oleh Dept. lain selain TI.

8.16.5 Cara mendapatkan dan memanfaatkan kapabilitas keamanan informasi yang disediakan oleh penyedia layanan *cloud*.

8.16.6 Cara mendapatkan keyakinan kendali keamanan informasi yang diimplementasikan oleh penyedia layanan *cloud*.

8.16.7 Cara mengelola kendali, antarmuka dan perubahan layanan ketika organisasi menggunakan beberapa layanan *cloud*, khususnya dari penyedia layanan *cloud* yang berbeda.

8.16.8 Prosedur penanganan insiden keamanan informasi yang terjadi terkait penggunaan layanan *cloud*.

8.16.9 Pendekatan untuk memantau, meninjau dan mengevaluasi penggunaan layanan *cloud* yang sedang berlangsung untuk mengelola risiko keamanan informasi.

8.16.10 Cara untuk mengubah penggunaan layanan *cloud*, termasuk strategi untuk berhenti

menggunakan layanan *cloud*.

8.17 Perencanaan dan Persiapan Manajemen Insiden Keamanan Informasi.

8.17.1 Setiap pengguna komputer baik SDM, mitra kerja atau pihak eksternal, secara pribadi bertanggung jawab untuk menjamin bahwa tindakannya tidak menyebabkan atau berpotensi menyebabkan kerawanan keamanan informasi.

8.17.2 Dept. TI Perusahaan harus menyediakan perangkat kerja untuk menindaklanjuti dan menyelesaikan setiap pelaporan insiden keamanan informasi secara cepat dan efektif.

8.18 Asesmen dan Keputusan tentang Peristiwa Keamanan Informasi.

8.18.1 Seluruh gangguan/insiden keamanan yang terjadi dan tindakan untuk mengatasinya akan dicatat dalam suatu basis data pelaporan insiden keamanan informasi, dan akan menjadi masukan dalam evaluasi manajemen keamanan informasi.

8.18.2 Koordinator Keamanan Teknologi Informasi harus mengevaluasi laporan dan penyelesaian insiden keamanan informasi untuk mengidentifikasi jenis, volume dan biaya yang terkait dalam rangka pengawasan dan evaluasi kinerja.

8.18.3 Semua data dan rekaman yang dibutuhkan untuk menganalisa dan menyelesaikan insiden keamanan informasi harus diamankan. Untuk insiden yang terkait dengan tindakan perdata atau pidana, pengamanan rekaman harus mengikuti peraturan dan hukum yang berlaku.

8.19 Respon terhadap Insiden Keamanan Informasi mencakup hal-hal sebagai berikut:

8.19.1 Pengurungan (*containing*) sistem yang terdampak insiden, jika konsekuensi dari insiden dapat menyebar.

8.19.2 Mengumpulkan bukti (*evidence*) sesegera mungkin setelah peristiwa terjadi.

8.19.3 Eskalasi, sebagaimana dipersyaratkan termasuk aktivitas manajemen krisis dan mungkin memerlukan rencana keberlangsungan bisnis.

8.19.4 Memastikan bahwa semua aktivitas respon yang terlibat tercatat dengan benar untuk analisis di kemudian hari.

8.19.5 Mengkomunikasikan keberadaan insiden keamanan informasi atau detail terkait kepada semua pihak internal dan eksternal terkait yang relevan.

8.19.6 Berkoordinasi dengan pihak internal dan eksternal seperti otoritas, grup dan forum kepentingan eksternal, pemasok dan klien untuk meningkatkan efektivitas respon dan membantu meminimalkan konsekuensi bagi organisasi lain.

8.19.7 Menutup peristiwa insiden yang telah berhasil ditangani dan menyimpan rekaman peristiwa insiden tersebut.

8.19.8 Melakukan analisis forensik keamanan informasi.

8.19.9 Melakukan analisis pasca-insiden untuk mengidentifikasi akar penyebab (*root cause*) masalah.

8.19.10 Mengidentifikasi dan mengelola kerentanan dan kelemahan keamanan informasi termasuk yang terkait dengan kendali yang telah menyebabkan, berkontribusi pada atau gagal mencegah terjadinya insiden.

8.20 Pembelajaran dari Insiden Keamanan Informasi.

Informasi yang diperoleh dari evaluasi insiden keamanan informasi digunakan untuk:

8.20.1 Meningkatkan rencana manajemen insiden termasuk skenario dan prosedur insiden.

8.20.2 Mengidentifikasi insiden berulang atau serius dan penyebabnya untuk memperbarui asesmen risiko keamanan informasi organisasi serta menentukan dan mengimplementasikan kendali tambahan yang diperlukan untuk mengurangi kemungkinan atau konsekuensi insiden serupa di masa depan.

8.20.3 Meningkatkan kesadaran dan pelatihan pengguna dengan menyediakan contoh apa yang terjadi, bagaimana merespon insiden tersebut, dan bagaimana menghindarinya di masa depan.

8.21 Pengumpulan bukti.

Dept. TI mengidentifikasi, mengumpulkan, menyimpan dan menyajikan bukti sesuai dengan berbagai tipe media penyimpanan, perangkat dan status peranti (baik menyala ataupun mati) terhadap pelanggaran keamanan informasi yang terjadi

8.22 Keamanan informasi selama terjadi suatu gangguan (disrupsi).

Perusahaan menerapkan dan memelihara:

8.22.1 Kendali keamanan informasi, sistem pendukung dan alat-alat dalam rencana keberlangsungan bisnis dan keberlangsungan TI.

8.22.2 Proses untuk memelihara kendali keamanan informasi yang ada selama disrupsi.

8.22.3 Kompensasi kendali untuk kendali keamanan informasi yang tidak dapat dijaga penerapannya selama disrupsi.

8.23 Kesiapan TI untuk keberlangsungan bisnis.

Dept. TI Perusahaan memastikan bahwa:

8.23.1 Struktur organisasi yang cukup telah disusun untuk mempersiapkan, memitigasi dan merespon disrupsi yang didukung oleh personil dengan tanggung jawab, otoritas dan kompetensi yang diperlukan.

8.23.2 Rencana keberlangsungan TI, termasuk prosedur respon dan pemulihan yang terperinci mengenai bagaimana organisasi berencana untuk mengelola disrupsi layanan TI:

a. dievaluasi secara reguler melalui latihan dan pengujian; dan

b. disetujui oleh SVP Transformasi Bisnis.

8.23.3 Rencana keberlangsungan TI meliputi informasi keberlangsungan TI berikut:

a. Spesifikasi kinerja dan kapasitas untuk memenuhi persyaratan dan sasaran

keberlangsungan bisnis sebagaimana ditentukan dalam BIA.

b. *Recovery Time Objective* (RTO) tiap-tiap layanan TI yang diprioritaskan dan prosedur untuk pemulihan komponen tersebut.

c. *Recovery Point Objective* (RPO) sumber daya TI yang diprioritaskan didefinisikan sebagai informasi dan prosedur untuk memulihkan informasi.

8.24 Persyaratan Legal, Statutori, Regulatori dan Kontraktual.

8.24.1 Dept. TI Perusahaan akan menjamin dipatuhinya kebijakan, pedoman, prosedur dan standar keamanan informasi di semua unit kerjanya dengan cara sebagai berikut:

a. Mengkomunikasikan kebijakan, pedoman dan prosedur yang terkait keamanan informasi ke seluruh SDM di setiap unit kerja.

b. Meningkatkan pengetahuan dan keterampilan SDM dalam hal pengelolaan keamanan informasi sesuai dengan bidang tugasnya.

c. Memeriksa dan mengevaluasi tingkat kepatuhan SDM terhadap pelaksanaan Pedoman ini secara berkala.

8.24.2 Setiap ketidakpatuhan terhadap kebijakan, pedoman, prosedur, dan standar keamanan informasi harus dicari penyebab utamanya dan ditindaklanjuti untuk mencegah terjadinya hal serupa di kemudian hari.

8.24.3 Seluruh SDM Perusahaan, dan pihak eksternal dilarang menggunakan perangkat lunak untuk menggandakan atau menggunakan lisensi secara tidak sah.

8.24.4 Rencana pemeriksaan kepatuhan teknis harus didokumentasikan, dikomunikasikan dan disetujui oleh VP Dept.TI.

8.24.5 Hasil-hasil pemeriksaan teknis harus dicatat dan dilaporkan sebagai masukan bagi evaluasi manajemen keamanan informasi.

8.25 Hak Kekayaan Intelektual.

8.25.1 Seluruh pengguna (*user*) sistem informasi milik Perusahaan termasuk pihak eksternal harus mematuhi Pedoman Pengelolaan Keamanan Informasi ini dan mentaati ketentuan hukum dan undang-undang yang terkait serta perjanjian tentang lisensi, termasuk persyaratan-persyaratan kontrak yang telah disetujui.

8.25.2 Dept. TI menjamin bahwa setiap ketentuan hukum dan perundang-undangan yang terkait dengan sistem informasi yang dimiliki Perusahaan akan diidentifikasi, didokumentasi dan dipelihara kemutakhirannya.

8.25.3 Dept. TI menjamin bahwa pemasangan perangkat lunak dalam sistem komputer milik Dept. TI dilakukan dengan mematuhi ketentuan penggunaan lisensi secara tepat. Penggandaan perangkat lunak secara tidak sah tidak diperbolehkan dan merupakan bentuk pelanggaran terhadap Pedoman Pengelolaan Keamanan Informasi ini serta ketentuan hak cipta.

8.25.4 Setiap penemuan, kegiatan, atau gagasan-gagasan praktis yang didapatkan/dihasilkan oleh SDM selama bekerja di Perusahaan dan dihasilkan oleh sumber daya milik Perusahaan adalah menjadi hak milik eksklusif Perusahaan.

8.25.5 Daftar lisensi perangkat lunak akan dipelihara dan diperbarui minimal setahun sekali.

8.25.6 Lisensi perangkat lunak yang disediakan oleh Dept. TI tidak boleh digunakan atau dipasang pada peralatan komputer selain milik Perusahaan.

8.25.7 Pemeriksaan berkala terhadap lisensi perangkat lunak yang terpasang akan dilakukan untuk memastikan bahwa Pedoman Keamanan Informasi ini telah diterapkan secara efektif.

8.26 Proteksi Rekaman.

8.26.1 Dept. TI mengeluarkan ketentuan tentang penyimpanan, penanganan rantai kustodi dan pemusnahan rekaman, yang mencakup pencegahan manipulasi rekaman, yang selaras dengan Pedoman Pengelolaan Arsip Dinamis .

8.26.2 Dept. TI menyusun jadwal retensi yang mendefinisikan rekaman dan periode waktu yang ditentukan untuk penyimpanannya.

8.26.3 Rekaman-rekaman penting milik Perusahaan dan/atau yang digunakan dan dihasilkan oleh sistem informasi/aset informasi yang dikelola Dept. TI seperti database, audit *log*, dan transaction *log* harus dilindungi dari kehilangan, kerusakan atau penyalahgunaan, sesuai peraturan atau undang-undang yang berlaku.

8.27 Privasi dan Proteksi Data Pribadi (PII).

8.27.1 Perusahaan akan melindungi kepemilikan dan kerahasiaan data pribadi baik pegawai internal, eksternal - dari mitra dan/atau *vendor* - dan data pribadi pelanggan (*customer*), selama yang bersangkutan masih memiliki hubungan kerja/usaha dengan Perusahaan.

8.27.2 Data pribadi tersebut hanya digunakan untuk kepentingan yang diperbolehkan oleh peraturan dan ketentuan perundang-undangan yang berlaku.

8.28 Tinjauan (*Review*) dan Kepatuhan terhadap Pedoman, Aturan dan Standar Keamanan Informasi.

8.28.1 Dept. TI merencanakan dan melaksanakan tinjauan independen secara periodik, yang mencakup asesmen peluang perbaikan berkelanjutan dan kebutuhan untuk perubahan pendekatan terhadap keamanan informasi.

8.28.2 Kegiatan peninjauan dilakukan oleh individu yang tidak memiliki kepentingan (independen) dengan area yang ditinjau dan memiliki kompetensi yang tepat untuk melakukan tinjauan.

8.28.3 Hasil tinjauan berupa rekaman yang dipelihara dan dilaporkan kepada manajemen yang meminta pelaksanaan kegiatan peninjauan.

8.28.4 Hak akses terhadap alat bantu tinjauan hanya boleh diberikan kepada administrator sistem yang bertanggung jawab untuk melindungi kerahasiaan dan mencegah penyalahgunaan alat bantu tinjauan yang digunakan.

8.29 Prosedur Operasi Terdokumentasi.

8.29.1 Dokumentasi dari sistem, baik yang tercetak ataupun yang berupa dokumen elektronik digolongkan sebagai dokumen rahasia dan harus disimpan secara aman serta hanya disediakan bagi mereka yang memerlukannya. Yang termasuk dokumentasi dari sistem antara lain struktur data, struktur jaringan, proses-proses otorisasi, dan sebagainya.

8.29.2 Dept. TI menjamin bahwa seluruh prosedur operasional yang terkait dengan penggunaan perangkat pengolah informasi dan komunikasi didokumentasikan, dirawat dan bisa didapatkan dengan mudah oleh SDM yang membutuhkannya.

8.29.3 Prosedur operasional harus berisikan antara lain:

a. Tata cara pengolahan dan penanganan informasi.
b. Tata cara menangani kesalahan-kesalahan atau kondisi khusus yang terjadi dilengkapi dengan pihak yang harus dihubungi bila mengalami kesulitan teknis.
c. Standard *Baseline Security Configuration* yang ditetapkan oleh Dept. TI, khusus untuk sumber daya informasi rahasia.
d. Cara memfungsikan kembali perangkat dan cara mengembalikan perangkat ke keadaan awal saat terjadi kegagalan sistem.
e. Tata cara *backup* serta pengelolaan catatan penggunaan (*audit trail*) dan catatan kejadian/kegiatan sistem (*system log*).

8.29.4 Perubahan terhadap fasilitas pengolah dan pengelola informasi harus dikendalikan. Dept. TI harus mempunyai catatan perubahan yang terdokumentasi, yang berisikan:

a. Identifikasi dan pencatatan perubahan yang berarti dan kajian atas potensi dampaknya.
b. Persetujuan formal yang mengikuti Prosedur Pengelolaan Perubahan yang berlaku.
c. Pemberitahuan perubahan ke seluruh SDM yang relevan.
d. Prosedur untuk menghentikan dan mengembalikan ke keadaan semula apabila terjadi kegagalan perubahan.

8.29.5 Pelaksanaan pengendalian perubahan harus merujuk kepada Prosedur Pengendalian Perubahan Layanan TI yang berlaku.

8.29.6 Jika pengelolaan fasilitas pengolah informasi diserahkan kepada Pihak Eksternal, Dept. TI harus menjamin dilakukannya evaluasi terhadap risiko dan ditetapkannya kendali-kendali untuk mengurangi setiap potensi kerusakan atau kehilangan data. Kendali-kendali ini harus disertakan dalam kontrak kerja.

9. PENGELOLAAN KENDALI KEAMANAN ORANG

9.1 Skrining.

9.1.1 Perusahaan akan melakukan penelitian dan pemeriksaan pada data pribadi dan

keterangan pekerjaan sebelumnya yang diberikan oleh SDM baru atau Pihak Eksternal, sesuai dengan Pedoman Penerimaan SDM / Pihak Eksternal yang berlaku.

9.2 Syarat dan Ketentuan Ketenagakerjaan.

9.2.1 Peran dan tanggung jawab SDM terhadap keamanan informasi harus menjadi bagian dari penjabaran tugas pokok dan fungsi, khususnya bagi mereka yang memiliki akses terhadap aset informasi yang bersifat rahasia dan berharga (mempunyai nilai nominal tertentu), dan rawan (mempunyai aspek nilai *intangible* atau terkait risiko keamanan terhadap aset informasi lainnya).

9.2.2 Peran dan tanggung jawab SDM dan Pihak Eksternal lainnya terhadap keamanan informasi didefinisikan, didokumentasikan dan dikomunikasikan kepada yang bersangkutan sebelum penugasan.

9.2.3 Seluruh SDM Perusahaan dan Pihak Eksternal lainnya wajib mematuhi Pedoman dan Prosedur Keamanan Informasi yang berlaku di Dept. TI Perusahaan.

9.3 *Awareness*, Pendidikan dan Pelatihan Keamanan Informasi.

9.3.1 Seluruh SDM Perusahaan yang menggunakan fasilitas TI harus mendapatkan pendidikan, pelatihan dan sosialisasi sistem keamanan informasi secara berkala sesuai tingkat tanggungjawabnya.

9.3.2 Pihak Eksternal jika diperlukan, mendapatkan sosialisasi untuk meningkatkan kepedulian terhadap keamanan informasi melalui proses induksi atau metode lain yang tepat.

9.4 Proses Kedisiplinan.

9.4.1 Kepatuhan SDM terhadap Pedoman dan Prosedur Keamanan Informasi harus ditinjau ulang secara berkala oleh atasan masing-masing dan menjadi bagian dari penilaian kinerja SDM.

9.4.2 SDM dan pihak eksternal yang melanggar Pedoman Keamanan Informasi yang berlaku di lingkungan Perusahaan akan dikenai sanksi atau tindakan disiplin sesuai ketentuan yang berlaku.

9.4.3 Koordinator Keamanan TI berhak untuk menghentikan/menutup untuk sementara atau selamanya hak menggunakan aset informasi bagi SDM yang sedang menjalani pemeriksaan yang terkait dengan dugaan adanya pelanggaran Pedoman Keamanan Informasi dan/atau yang sedang menjalani proses hukum.

9.5 Tanggungjawab setelah Terminasi atau Perubahan Pekerjaan.

9.5.1 Sebelum penghentian, pemutusan hubungan kerja, atau mutasi efektif berlaku, Perusahaan wajib mengingatkan hak dan kewajiban SDM dan Pihak Eksternal untuk tetap mematuhi Pedoman dan aturan keamanan informasi yang berlaku di Perusahaan terutama yang terkait dengan kewajiban menjaga kerahasiaan.

9.5.2 SDM dan Pihak Eksternal yang telah berhenti bekerja atau habis masa kontrak kerjanya harus mengembalikan seluruh aset milik Perusahaan yang dipergunakan selama bekerja di Perusahaan.

9.5.3 SDM berkeahlian khusus atau yang berada di posisi kunci harus didorong agar melakukan alih keahlian dan pengetahuannya (*transfer of knowledge*) kepada rekan kerjanya sebelum mereka meninggalkan Perusahaan.

9.5.4 Hak akses terhadap sistem informasi yang dimiliki SDM dan Pihak Eksternal akan dicabut secara otomatis bila yang bersangkutan tidak lagi bekerja di Perusahaan.

9.6 Perjanjian Kerahasiaan.

9.6.1 SDM dan Pihak Eksternal yang akan menggunakan aset informasi milik dan/atau yang dikelola Dept. TI harus menyetujui dan menandatangani ketentuan penggunaan aset yang berlaku di Perusahaan.

9.6.2 SDM dan Pihak Eksternal yang akan menggunakan aset informasi yang tergolong rahasia dan terbatas terlebih dahulu harus menyetujui dan menandatangani Pernyataan Menjaga Kerahasiaan (*Non-Disclosure Agreement*) sebelum memulai pekerjaan atau kerja sama dengan Perusahaan.

9.6.3 Sebelum dilakukan penghapusan hak akses dan/atau akun mantan SDM harus dipastikan bahwa segala isi akun sudah diarsipkan sehingga bisa diakses kembali bila situasi memerlukannya.

9.7 Bekerja Jarak Jauh (*Teleworking*).

9.7.1 Kegiatan *teleworking* hanya akan diizinkan kepada SDM yang bersangkutan bila memenuhi syarat-syarat sebagai berikut:

a. Lokasinya memenuhi persyaratan keamanan informasi.
b. Mematuhi Ketentuan Keamanan Informasi.
c. Mendapat persetujuan VP Unit Kerja yang bersangkutan dan VP Dept. TI Perusahaan.

9.7.2 SDM yang diizinkan untuk melakukan kegiatan *teleworking* harus menandatangani surat perjanjian untuk mencegah akses tidak berwenang oleh keluarga, teman, tamu atau pihak yang tidak berwenang lainnya.

9.8 Pelaporan Kejadian Keamanan Informasi.

9.8.1 Setiap SDM dan Pihak Eksternal yang mendeteksi adanya virus atau masalah lainnya dalam penggunaan layanan TI wajib segera melaporkannya kepada Dept. TI.

9.8.2 Kejadian pelanggaran terhadap kerahasiaan, keutuhan dan ketersediaan informasi harus dilaporkan kepada Dept. TI Perusahaan.

10. PENGELOLAAN KENDALI KEAMANAN FISIK

10.1 Perimeter Keamanan Fisik.

10.1.1 Kantor, ruangan, dan fasilitas yang berisikan informasi rahasia harus memiliki pengamanan fisik yang memadai. Pintu dan jendela harus dikunci jika ditinggalkan.

10.1.2 Ruang Server, *Data Center* (DC) dan *Disaster Recovery Center* (DRC) harus diamankan dengan menggunakan dinding permanen yang tidak dapat dijebol tanpa alat bantu.

10.1.3 Penempatan fasilitas penyimpanan dan pengolah informasi harus ditempatkan secara aman dan terlindungi dari gangguan fisik.

10.2 Entri Fisik.

10.2.1 Seluruh SDM dan Pihak Eksternal yang memasuki lingkungan Perusahaan harus mengenakan kartu identitas (*ID Card*) resmi yang dikeluarkan Perusahaan serta pencatatan terhadap jam masuk dan keluarnya.

10.2.2 Seluruh SDM dan Pihak Eksternal yang memasuki fasilitas *Data Center* (DC) atau area kerja yang berisikan aset informasi yang bersifat rahasia, harus didampingi SDM Dept. TI yang berwenang. Waktu masuk dan keluar serta maksud kedatangan harus dicatat dalam buku catatan keluar masuk ruangan (*log book*) serta wajib mematuhi seluruh ketentuan yang berlaku pada fasilitas atau area tersebut.

10.3 Pengamanan Kantor, Ruangan dan Fasilitas.

10.3.1 Perangkat pengolah informasi harus ditempatkan di lokasi yang tidak dilewati / dilalui oleh Pihak Eksternal.

10.3.2 Perangkat pengolah informasi termasuk mesin faksimili, printer atau komputer yang digunakan untuk memproses informasi rahasia harus ditempatkan di lokasi yang aman untuk mencegah kebocoran informasi tersebut ke pihak yang tidak berwenang.

10.3.3 Ruang Server, *Data Center* (DC) dan *Disaster Recovery Center* (DRC) tidak boleh digunakan untuk ruang kerja, kecuali dalam rangka melakukan pemeliharaan, perbaikan atau instalasi perangkat TI baru dan harus ada didampingi oleh SDM Dept. TI yang berwenang.

10.3.4 Pengambilan gambar di Ruang Server, *Data Center* (DC) dan *Disaster Recovery Center* (DRC) harus dengan seizin penanggung jawab ruangan.

10.3.5 Akses keluar masuk fasilitas Ruang Server, *Data Center* (DC), *Disaster Recovery Center* (DRC) dan area kerja lainnya yang berisikan aset informasi yang bersifat rahasia dan sangat rahasia harus dibatasi dan hanya diberikan kepada SDM tertentu yang berwenang.

10.4 Pemantauan Keamanan Fisik.

10.4.1 Area keluar masuk barang dan area lainnya (pengembangan) harus selalu dijaga, diawasi, dan dikendalikan, dan jika mungkin diisolasi dari fasilitas pengolah informasi (komputer) untuk menghindari akses oleh pihak yang tidak berwenang.

10.5 Perlindungan dari Ancaman Fisik dan Lingkungan.

10.5.1 Area yang digunakan untuk menyimpan aset informasi penting (Ruang Arsip, Ruang Server, *Data Center* (DC), *Disaster Recovery Center* (DRC), Ruang Alat Komunikasi atau Ruang Penyimpanan Media) harus mendapatkan perlindungan yang layak dari dampak lingkungan/polusi, dengan aliran udara (ventilasi), suhu, dan kelembaban yang sesuai.

10.5.2 Sistem perlindungan kebakaran harus dipasang dengan aman, tidak membahayakan personil yang bekerja di fasilitas Ruang Server, *Data Center* (DC) atau *Disaster Recovery Center* (DRC) serta dirawat secara teratur untuk melindungi fasilitas dan perangkat yang ada di dalamnya.

10.5.3 Fasilitas untuk melindungi perangkat pengolah informasi dari petir harus dipasang pada semua unit kerja Dept. TI.

10.6 Bekerja di Area yang Aman.

10.6.1 SDM dan Pihak Eksternal hanya diperbolehkan untuk bekerja pada lokasi yang telah ditentukan.

10.6.2 Makanan dan minuman dilarang untuk dibawa masuk ke atau dikonsumsi di dalam ruang bekerja.

10.6.3 Semua area yang digunakan untuk menyimpan aset informasi penting adalah area bebas rokok.

10.7 Meja Rapi dan Layar Bersih.

10.7.1 Komputer yang berisikan informasi penting harus dipasang *screen lock* yang aktif dengan sendirinya setelah komputer tidak digunakan pada jangka waktu tertentu setidaknya selama 5 (lima) menit dan untuk membukanya dibutuhkan *login* dan *password* dari pengguna (*User*).

10.7.2 Komputer yang tidak terawasi dan ditinggalkan dalam jangka waktu tertentu setidaknya lebih dari 30 (tigapuluh) menit harus dengan sendirinya memutuskan sesi kerjanya dan/atau mematikan sistemnya *(sleep/hibernate*).

10.7.3 Informasi rahasia harus dijauhkan dari penglihatan pihak yang tidak berwenang, tidak diletakkan di atas meja kerja secara sembarangan, dan harus disimpan di lemari yang dikunci apabila tidak digunakan, khususnya pada kondisi meja sedang ditinggalkan.

10.7.4 Setelah selesai menggunakan papan tulis (*whiteboard*/media presentasi), maka informasi didalamnya harus dihapus jika mengandung informasi sensitif atau rahasia, untuk menghindari terbaca oleh orang yang tidak berwenang.

10.7.5 Pengguna tidak boleh meninggalkan kertas, dokumen, dan buku yang mengandung informasi rahasia atau sensitif di meja kerja (*Clear Desk*), printer, mesin fotokopi atau mesin fax untuk menghindari terbaca oleh orang yang tidak berwenang.

10.7.6 Kertas hasil kesalahan dalam penggunaan printer, mesin fotokopi atau mesin fax harus dihancurkan menggunakan *paper shredder* jika mengandung informasi rahasia.

10.8 Penempatan dan Perlindungan Peralatan.

10.8.1 Dept. TI menyimpan *server*, infrastruktur jaringan dan komunikasi, serta fasilitas pengolah dan pengelola informasi rahasia lainnya di ruangan khusus (Ruang Server, *Data Center* (DC) atau *Disaster Recovery Center* (DRC)) yang dilindungi dengan pengamanan fisik yang memadai dan berfungsi dengan baik seperti pintu elektronik, sistem pemadam kebakaran, alarm bahaya dan perangkat pemutus aliran listrik.

10.8.2 Batas minimum dan maksimum untuk suhu dan kelembaban di dalam Ruang Server, *Data Center* (DC) atau *Disaster Recovery Center* (DRC) ditetapkan dengan memperhatikan persyaratan lingkungan operasional perangkat. Kondisi suhu dan kelembaban ini harus dipantau secara berkala.

10.9 Keamanan Aset di luar Lokasi.

10.9.1 SDM dan Pihak Eksternal dilarang keras untuk meninggalkan peralatan dan media penyimpanan informasi di tempat umum atau area yang tidak aman.

10.9.2 Dept. TI menerapkan pelacakan lokasi dan kemampuan untuk mengendalikan dan menghapus data dan informasi yang terdapat di dalam perangkat *mobile* dari jarak jauh.

10.10 Media Penyimpanan.

10.10.1 Seluruh media penyimpan informasi mudah jinjing (*removable*) yang sudah tidak terpakai lagi, harus diformat ulang atau dihapus isinya sebelum dibuang. Tetapi jika hal itu tidak bisa dilakukan, maka media tersebut harus dihancurkan.

10.10.2 Media kertas termasuk *carbon copies* dan cetakan printer yang mengandung informasi rahasia yang sudah tidak terpakai lagi, harus dihancurkan dengan menggunakan alat penghancur kertas atau dibakar.

10.10.3 Media Penyimpanan seperti CD, DVD, *flash disk*, dan lain-lain disimpan dalam laci yang terkunci terutama pada saat tidak digunakan.

10.11 Utilitas Pendukung.

10.11.1 Semua perangkat pengolah informasi harus mendapatkan pasokan daya yang sesuai dengan spesifikasi yang disyaratkan oleh pabrikan perangkat. Untuk setiap lokasi kerja terutama Ruang Server, *Data Center* (DC) atau *Disaster Recovery Center* (DRC) tersedia pasokan listrik yang cukup untuk beban maksimal seluruh perangkat, termasuk perangkat pendukung yang ada di lokasi tersebut.

10.11.2 Pasokan listrik yang digunakan untuk mengoperasikan perangkat pengolah informasi Perusahaan harus mempunyai sumber alternatif dengan daya dan jangka waktu ketersediaan atau jangka waktu pengoperasian yang cukup. Pasokan ini minimal berupa

perangkat generator listrik dan perangkat UPS (*Uninterruptable Power Supply*) dengan daya yang cukup dan dengan konfigurasi yang dapat memindahkan pasokan listrik tanpa gangguan terhadap perangkat komputer/server.

10.11.3 Instalasi jaringan listrik harus sesuai dengan standar instalasi jaringan listrik dan standar keselamatan yang berlaku.

10.12 Keamanan Pengkabelan.

10.12.1 Konfigurasi jaringan kabel data dan daya harus terekam dalam dokumen resmi yang dimutakhirkan untuk setiap perubahan.

10.12.2 Jaringan kabel data harus dipisahkan dari jaringan kabel listrik, dengan jarak yang cukup untuk menghindari dampak radiasi (elektromagnet), dan dengan pencantuman label yang sesuai.

10.12.3 Jaringan kabel data atau koneksi yang menghubungkan perangkat komputer/server yang penting, harus diamankan melalui:

a. Konstruksi jalur kabel data yang dapat melindungi kabel dari dampak lingkungan atau pihak yang tidak berwenang.
b. Spesifikasi kabel data yang sesuai dengan ancaman lingkungan (air, suhu/panas, debu/ kotoran atau radiasi).
c. Penempatan yang terlindung dari ancaman fisik disekitarnya (jalur lintas kendaraan, peralatan berat, atau pekerjaan konstruksi).
d. Proses inspeksi dan perawatan rutin.

10.12.4 Jaringan kabel data harus memiliki label pada setiap ujungnya dengan detail sumber dan tujuan yang cukup untuk memungkinkan identifikasi fisik dan inspeksi kabel.

10.13 Pemeliharaan Peralatan.

10.13.1 Seluruh perangkat pengolah informasi penting dan peralatan pendukung harus diperiksa dan diujicoba efektivitasnya secara teratur/berkala, dirawat dan dibersihkan sesuai dengan spesifikasi pabrikannya.

10.13.2 Perawatan dan perbaikan perangkat pengolah informasi hanya boleh dilakukan oleh personil yang berwenang dan mempunyai kompetensi teknis yang sesuai.

10.13.3 Dept. TI harus memastikan bahwa pihak eksternal sebagai penyedia layanan memelihara kemampuannya dalam menyediakan layanan yang telah ditetapkan.

10.13.4 Keluar masuk perangkat di Ruang Server, *Data Center* (DC) atau *Disaster Recovery Center* (DRC) harus didokumentasikan dan disetujui oleh SDM yang berwenang.

10.13.5 Keluar masuk perangkat untuk keperluan perawatan dan perbaikan di luar Dept. TI harus didokumentasikan dan mendapatkan izin dari SDM yang berwenang.

10.14 Pemusnahan atau Penggunaan Kembali Peralatan dengan Aman.

Dalam hal penggunaan kembali atau pemindahan media penyimpanan kepada pihak di luar organisasi, maka harus memenuhi ketentuan sebagai berikut:

10.14.1 Media penyimpanan yang berisi informasi rahasia harus dihancurkan, dihapus atau ditimpa dengan menggunakan teknik yang membuat informasi asli tidak dapat diambil kembali.

10.14.2 Media penyimpanan yang berisi informasi sangat rahasia harus dihancurkan secara fisik.

11. PENGELOLAAN KENDALI KEAMANAN TEKNOLOGI

11.1 Perangkat *User End Point*.

11.1.1 Fasilitas *mobile computing* yang disediakan oleh Dept. TI hanya boleh digunakan untuk melaksanakan tugas pokok dan fungsi sesuai posisi, dan harus disetujui oleh VP Dept. TI.

11.1.2 Penerima fasilitas *mobile computing* Perusahaan harus menjamin bahwa akses ke perangkat yang digunakan akan dilindungi dari pihak yang tidak berwenang.

11.1.3 Dept. TI menjamin bahwa SDM yang menggunakan fasilitas *mobile computing* akan mendapatkan pelatihan yang memadai dan harus sadar akan risiko-risiko keamanan yang terus meningkat terhadap informasi yang disimpan di dalam peralatan-peralatan yang digunakan.

11.1.4 Akses *Wireless Access Point* (WAP) hanya boleh disediakan oleh Dept. TI Perusahaan.

11.1.5 Jaringan WAP akan dipantau secara berkala untuk memeriksa kelemahan dan mendeteksi adanya penggunaan yang tidak sesuai dengan prosedur yang ditetapkan. Dept.TI berhak untuk mengisolasi dan/atau melepas perangkat WAP yang tidak terdaftar atau tidak diotorisasi oleh Dept. TI Perusahaan.

11.2 Hak Akses Istimewa (*Privilege*).

11.2.1 Setiap pengguna akan diidentifikasi kebutuhan hak akses istimewanya untuk setiap sistem atau proses.

11.2.2 Dept. TI memelihara proses otorisasi persetujuan hak akses istimewa dan rekaman semua alokasi hak akses istimewa.

11.2.3 Penggunaan identitas dengan Hak Akses Istimewa hanya diperuntukkan bagi tugas-tugas administratif yang bukan merupakan tugas harian.

11.3 Pembatasan Akses Informasi.

11.3.1 Dept. TI harus menjamin bahwa akses terhadap informasi hanya diberikan bagi mereka yang memerlukan akses dalam menjalankan pekerjaannya.

11.3.2 Informasi yang penting dan rawan yang dikelola oleh Dept. TI harus disimpan di lingkungan komputer terpisah agar tidak dapat digunakan oleh pihak yang tidak berwenang.

11.4 Akses ke Kode Sumber (*Source Code*).

11.4.1 Pengelolaan akses ke kode sumber program beserta acuan pustaka (*library*) sesuai

dengan program yang telah ditetapkan.

11.4.2 Akses terhadap kode sumber tidak dipegang langsung oleh *Developer*, namun melalui alat (*tools*) yang mengendalikan aktifitas dan otorisasi pada kode sumber.

11.4.3 *Log audit* dari semua akses dan perubahan pada kode sumber harus dipelihara dengan baik.

11.5 Autentikasi Aman.

Implementasi *log* sistem atau aplikasi didesain untuk meminimalkan risiko akses yang tidak sah (*unathorized*) dengan mempertimbangkan hal-hal berikut:

11.5.1 Tidak menampilkan pesan bantuan, sistem sensitif atau informasi aplikasi selama prosedur *log* masuk sampai proses *log-on* berhasil diselesaikan.

11.5.2 Memvalidasi informasi *log* masuk hanya setelah menyelesaikan semua data input.

11.5.3 Memproteksi terhadap upaya *brute force log* masuk pada nama pengguna dan kata sandi dengan memblokir pengguna setelah mencapai jumlah maksimum kegagalan upaya masuk.

11.5.4 Tidak menampilkan kata sandi dalam teks yang jelas saat dimasukkan.

11.5.5 Tidak mentransmisikan kata sandi dalam teks yang jelas melalui jaringan agar tidak tertangkap oleh program *sniffer* jaringan.

11.5.6 Mematikan sesi yang tidak aktif setelah mencapai periode yang ditentukan, terutama di lokasi berisiko tinggi seperti area publik atau eksternal di luar manajemen keamanan organisasi atau pada peranti titik akhir pengguna.

11.5.7 Membatasi durasi waktu terhubung untuk memberikan keamanan tambahan untuk aplikasi berisiko tinggi dan mengurangi peluang akses yang tidak sah.

11.6 Manajemen Kapasitas.

11.6.1 Dept. TI memantau penggunaan kapasitas sistem informasi seperti *file server*, *email/web server*, infrastruktur *network* dan sistem lainnya yang kritikal bagi kegiatan perusahaan serta membuat proyeksi kebutuhan kapasitas ke depan, termasuk kebutuhan lisensi perangkat, untuk menjamin ketersediaan sistem informasi yang diperlukan.

11.6.2 Perencanaan dan pemantauan kapasitas sistem informasi merujuk kepada Prosedur Pengelolaan Kapasitas yang ditetapkan tersendiri.

11.7 Proteksi terhadap Perangkat Perusak (*Malware*).

11.7.1 Untuk mencegah dan mengurangi risiko masuknya *virus*, setiap komputer milik perusahaan harus dipasang perangkat lunak *antivirus* yang dijaga kemutakhirannya secara berkala.

11.7.2 Setiap surat elektronik (*email*) yang dikirim atau diterima melalui server perusahaan harus dipastikan tidak berisikan virus atau program lain yang membahayakan.

11.7.3 Setiap pengguna komputer perusahaan harus memastikan bahwa lampiran (*attachment*)

email, *file* yang diunduh dari Internet dan yang disalin dari dan/atau ke media penyimpan informasi (*flash disk*, CD/DVD, *tape*, *portable hard disk*) bebas dari *virus* dan/atau program lain yang membahayakan.

11.8 Manajemen Kerentanan Teknis (*Vulnerability*).

11.8.1 Dept. TI akan memantau kelemahan teknis (*technical vulnerability*) dan ketersediaan *security patch* terkini dari *vendor* atau sumber lain yang terverifikasi.

11.8.2 Semua *server* atau perangkat perusahaan yang kritikal/penting harus menerapkan *security patch* terkini segera setelah hal itu tersedia. Sebelum diterapkan di lingkungan operasional, risiko penerapan *security patch* perlu dikaji dan dilakukan pengujian pada fasilitas pengembangan (*development*) untuk memastikan agar penerapannya tidak menyebabkan gangguan terhadap operasional layanan TI. Sedangkan untuk *server* atau perangkat yang non-kritikal penerapan *security patch* dapat dilakukan sesuai kebutuhan.

11.8.3 Penerapan *security patch* harus dilakukan dengan mengikuti prosedur pengelolaan perubahan (*change management*) yang berlaku.

11.8.4 Bukti penerapan *security patch* harus disimpan sebagai rekaman.

11.8.5 Seluruh SDM dan Pihak Eksternal dilarang melakukan kegiatan melacak dan menemukan *password*, mengidentifikasi kelemahan keamanan informasi, membuka enkripsi file dan/atau menggunakan perangkat lunak maupun perangkat keras yang dapat dioperasikan untuk mengevaluasi atau menerobos keamanan sistem informasi, kecuali mendapat ijin dan diberi wewenang oleh VP Dept. TI Perusahaan.

11.8.6 Pemeriksaan kepatuhan teknis seperti tes penetrasi (*penetration test*), pemindaian jaringan (*scanning*) atau teknik pencarian kelemahan keamanan informasi lainnya, akan dilakukan secara berkala oleh SDM yang memiliki kompetensi pada bidangnya baik dari internal Perusahaan ataupun menggunakan jasa ahli independen dari luar Perusahaan.

11.9 Manajemen Konfigurasi.

11.9.1 Konfigurasi perangkat keras, perangkat lunak, layanan, dan jaringan yang telah ditetapkan direkam sebagai *log*, dipelihara dari semua perubahan konfigurasi dan disimpan dengan aman.

11.9.2 Perubahan pada konfigurasi mengikuti ketentuan pada Instruksi Kerja aplikasi manajemen konfigurasi yang berlaku.

11.9.3 Catatan konfigurasi setidaknya memuat catatan tentang:

a. Pemilik terbaru atau kontak informasi terkait aset.
b. Tanggal perubahan konfigurasi terakhir.
c. Versi *template* konfigurasi.
d. Terkait dengan konfigurasi aset lainnya.

11.10 Penghapusan Informasi.

11.10.1 Informasi yang terkandung dalam media penyimpan informasi yang bisa dipakai ulang dan digunakan sebagai media transit seperti disket, USB *flash disk* dan *portable harddisk* harus dihapus jika tidak lagi diperlukan, namun hanya dilakukan jika salinan asli informasi tersebut masih tersedia.

11.10.2 SDM yang diminta untuk menghapus dan memindahkan informasi melalui media apapun harus sadar/peduli terhadap kebijakan keamanan informasi yang berlaku di Perusahaan dan memahami prosedur-prosedur yang harus dijalankan.

11.11 Penyamaran (*masking*) Data.

11.11.1 Penerapan teknik penyamaran data meliputi namun tidak terbatas pada hal-hal berikut ini:

a. Tidak memberikan semua pengguna akses ke semua data, oleh karena itu perlu mendesain *query* dan samaran untuk hanya menampilkan data minimum yang diperlukan kepada pengguna.
b. Mendesain dan mengimplementasikan mekanisme untuk mengaburkan data yang tidak diperlukan untuk dilihat oleh personil yang tidak berwenang.
c. Persyaratan legal atau regulatori yang harus dipatuhi terkait hal ini.

11.11.2 Penggunaan teknik penyamaran data, pseudonimisasi, atau anonimisasi akan terkait dengan hal-hal berikut ini:

a. Level kekuatan penyamaran data, pseudonimisasi atau anonimisasi sesuai dengan penggunaan data yang diproses.
b. Kendali akses ke data yang diproses.
c. Perjanjian atau pembatasan penggunaan data yang diproses.
d. Melarang penyusunan data yang diproses dengan informasi lain sehingga dapat mengidentifikasi PII *principal*.
e. Melacak penyediaan dan penerimaan data yang diproses.

11.12 Pencegahan Kebocoran Data.

Dept. TI akan melakukan hal-hal berikut ini untuk mengurangi risiko kebocoran data:

11.12.1 Mengidentifikasi dan mengklasifikasi informasi untuk memproteksi kebocoran.

11.12.2 Memantau saluran kebocoran data (*email*, *file transfer*, *mobile device*) dimana memungkinkan untuk dilakukan.

11.12.3 Mengambil langkah-langkah yang diperlukan untuk mencegah kebocoran informasi lebih lanjut.

11.13 Pencadangan Informasi.

11.13.1 Seluruh informasi penting dan rawan yang dikelola oleh Dept. TI harus dibuat salinannya (*backup*) secara berkala untuk menjamin keutuhan dan ketersediaannya saat diperlukan.

11.13.2 Data yang disimpan di *server* jaringan akan dibuat salinannya sesuai dengan prosedur *backup* dan seluruh *backup* akan disimpan secara aman di lokasi yang terpisah.

11.13.3 Secara berkala hasil salinan harus diperiksa keutuhan dan ketersediaannya.

11.14 Redundansi Fasilitas Pemrosesan Informasi.

Dept. TI menerapkan sistem redundan sebagai berikut:

11.14.1 Kontrak dengan dua atau lebih pemasok jaringan dan fasilitas pemrosesan informasi kritikal seperti penyedia layanan internet.

11.14.2 Menggunakan jaringan redundan.

11.14.3 Menggunakan dua pusat data yang terpisah secara geografis dengan sistem pencadangan data *mirrored*.

11.14.4 Menggunakan catu daya atau sumber daya redundan secara fisik.

11.14.5 Menggunakan beberapa bagian paralel komponen perangkat lunak, dengan penyeimbangan beban otomatis di antaranya (antara bagian di pusat data yang sama atau di pusat data yang berbeda).

11.14.6 Memiliki komponen terduplikat dalam sistem (seperti CPU, *harddisk*, memori) atau dalam jaringan (misalnya *firewall*, *router*, *switch*).

11.15 Pembuatan *Log*.

11.15.1 Prosedur pemantauan penggunaan sistem pengolah informasi akan ditetapkan tersendiri untuk menjamin agar kegiatan yang tidak berwenang tidak terjadi. Prosedur ini harus menjamin pemeriksaan terhadap:

a. Kegagalan akses (*access failures*).
b. Pola-pola *logon* yang mengindikasikan penggunaan yang tidak wajar.
c. Alokasi dan penggunaan hak akses khusus (*privileged access capability*).
d. Penelusuran transaksi dan pengiriman *file* tertentu yang mencurigakan.
e. Penggunaan perintah (*command*) penting/kritikal.

11.15.2 Akses terhadap *audit log* harus dilindungi dari perubahan atau penghapusan. *System Administrator* tidak boleh memiliki kemampuan menghapus atau menonaktifkan *log* aktivitas mereka sendiri.

11.15.3 Aktivitas *System Administrator* dan *System Operator* juga harus di *log*.

11.15.4 Semua *log* harus dilindungi, dievaluasi dan dianalisa secara berkala minimum 1 (satu) tahun sekali.

11.15.5 Gangguan keamanan informasi yang ditemukan selama pemantauan *log* harus segera dicatat dan dilaporkan, sesuai Prosedur Pengelolaan Insiden Keamanan TI.

11.16 Pemantauan Aktivitas.

11.16.1 Dept. TI melakukan pemantauan sistem yang meliputi namun tidak terbatas pada:

a. Jaringan keluar dan masuk, lalu lintas sistem dan aplikasi.
b. Akses ke sistem, server, peralatan jaringan, sistem pemantauan, aplikasi kritikal dan lain-lain.
c. Sistem level kritikal atau admin dan *file* konfigurasi jaringan.
d. *Log* dari alat keamanan (*antivirus*, *intrusion detection/prevention system, filter web, firewall*, pencegahan kebocoran data dan lain-lain).
e. *Log* peristiwa yang berkaitan dengan aktivitas sistem dan jaringan.
f. Memeriksa bahwa kode yang dieksekusi telah terotorisasi untuk berjalan dalam sistem dan bahwa kode tersebut tidak dirusak.
g. Penggunaan sumber daya (cpu, *hard disk, memori, bandwidth*) beserta kinerjanya.

11.16.2 Dept. TI menetapkan acuan *baseline* keadaan normal dan melakukan pemantauan terhadap anomali. Penetapan *baseline* ini dengan mempertimbangkan:
a. Meninjau pemanfaatan sistem pada periode normal dan puncak.
b. Waktu, lokasi dan frekuensi akses untuk setiap pengguna atau kelompok pengguna.

11.16.3 Sistem pemantauan dikonfigurasi terhadap acuan *baseline* yang telah ditetapkan untuk mengidentifikasi perilaku anomali, seperti:
a. Terminasi proses atau aplikasi yang tidak direncanakan.
b. Aktivitas yang biasanya terkait dengan perangkat perusak atau lalu lintas yang berasal dari alamat IP atau domain berbahaya yang diketahui (suatu *Command-and-Control* (C&C) *Server* yang memiliki sebuah *malicious network* yang dapat juga disebut sebagai *botnet*).
c. Karakteristik serangan yang diketahui (*denial of service*, *buffer overflows*).
d. Perilaku sistem yang tidak biasa (pemberlakuan *log keystroke*, injeksi proses dan deviasi dalam penggunaan protokol standar).
e. Kemacetan (*bottleneck*) dan kelebihan beban (*overloads*) (antrian jaringan, level latensi, dan *jitter* jaringan).
f. Akses tidak sah / *unauthorized* (aktual atau percobaan) ke sistem atau informasi.
g. Pemindaian aplikasi bisnis, sistem, dan jaringan yang tidak sah / *unauthorized*.
h. Upaya yang berhasil ataupun gagal dalam mengakses sumber daya yang diproteksi (*server* DNS, *portal web*, *file systems*).
i. Perilaku pengguna dan sistem yang tidak biasa dalam kaitannya dengan perilaku yang diharapkan.

11.17 Sinkronisasi Jam.

11.17.1 Seluruh sistem pengolahan informasi harus dikonfigurasi dengan tanggal dan jam yang sama dan disinkronkan dengan sumber waktu yang akurat dengan *server Network Time*

Protocol (NTP) atau metode lain.

11.18 Penggunaan Program Utilitas *Privilege*.

Dept. TI mengatur dan melakukan pemantauan terhadap hal-hal berikut ini:

11.18.1 Alat bantu pengembangan seperti *compiler* atau *editor* dan alat bantu sistem (*system utilities*) tidak boleh dipasang dan diakses di perangkat operasional.

11.18.2 Pembatasan penggunaan program utilitas kepada jumlah minimum pengguna resmi yang terotorisasi.

11.18.3 Penggunaan prosedur identifikasi, autentikasi dan otorisasi untuk program utilitas, termasuk identifikasi unik dari orang yang menggunakan program utilitas.

11.18.4 Mendefinisikan dan mendokumentasikan level otorisasi untuk program utilitas.

11.18.5 Otorisasi untuk penggunaan program utilitas secara *ad hoc*.

11.18.6 Tidak mengizinkan program utilitas bagi pengguna yang memiliki akses ke aplikasi pada sistem yang mempersyaratkan segregasi tugas.

11.18.7 Menghapus atau menonaktifkan semua program utilitas yang tidak diperlukan.

11.18.8 Membatasi ketersediaan program utilitas.

11.18.9 Membuat *log* semua penggunaan program utilitas.

11.18.10 Penggunaan alat bantu baik perangkat lunak maupun perangkat keras untuk mengetahui kelemahan keamanan informasi, memindai (*scanning*) *password*, atau untuk melemahkan dan menerobos sistem keamanan informasi tidak diizinkan kecuali atas persetujuan tertulis VP Dept. TI Perusahaan.

11.19 Instalasi Perangkat Lunak pada Sistem Operasional.

11.19.1 Dept. TI menetapkan daftar perangkat lunak berlisensi dan/atau perangkat lunak *open source* yang boleh dipasang di perangkat keras perusahaan.

11.19.2 Pemasangan (instalasi) perangkat lunak di perangkat keras milik perusahaan hanya boleh dilakukan oleh pegawai Dept. TI yang berwenang atau personil alih daya (*outsourcing*) yang ditugaskan.

11.20 Keamanan Jaringan.

11.20.1 Kegiatan jaringan akan dipantau untuk menjamin bahwa sumber daya jaringan digunakan secara efektif dan efisien, dan agar tidak terjadi kesalahan pemrosesan.

11.20.2 Penyambungan atau perluasan jaringan komputer dan akses ke sistem jaringan internal atau eksternal ditentukan berdasarkan kebutuhan kegiatan Perusahaan dan dikendalikan serta diatur oleh Dept. TI. Persetujuan perluasan jaringan baik internal maupun eksternal hanya dapat diberikan oleh VP Dept. TI Perusahaan.

11.20.3 Setiap sistem yang mengandung aplikasi penting yang dikelola Dept. TI atau yang memberi akses ke informasi yang rahasia, harus dipasangi perangkat *firewall* untuk melindungi dari

akses oleh pihak yang tidak berwenang.

11.21 Keamanan Layanan Jaringan.

11.21.1 Wewenang pengguna untuk memasuki jaringan komputer harus dibatasi sesuai dengan layanan yang secara resmi telah ditetapkan.

11.21.2 Akses ke internet diizinkan dalam rangka mendukung pelaksanaan kegiatan Perusahaan serta untuk meningkatkan kompetensi dan pengetahuan SDM.

11.21.3 Akses ke internet harus menggunakan perangkat lunak yang aman dan melalui *gateway* internet yang telah ditetapkan.

11.21.4 Akses oleh pihak eksternal ke jaringan Perusahaan hanya diberikan dalam rangka pelaksanaan kegiatan Perusahaan, serta diberikan setelah perjanjian kontrak dan Pernyataan Menjaga Kerahasiaan disetujui oleh pihak eksternal.

11.21.5 Hak akses pihak eksternal yang diizinkan masuk ke jaringan Perusahaan harus dirinci secara jelas, dan kegiatannya selama menggunakan jaringan akan dipantau, diawasi, dan dicatat.

11.22 Segregasi Jaringan.

11.22.1 Fasilitas pengembangan dan pengujian (*testing*), sedapat mungkin dipisahkan dari fasilitas untuk operasional.

11.22.2 Alat bantu pengembangan seperti *compiler* atau *editor* dan alat bantu sistem (*system utilities*) tidak boleh dipasang pada perangkat operasional.

11.22.3 Arsitektur jaringan harus didokumentasikan secara jelas dan terinci, termasuk pengaturan (*setting*) yang direncanakan bagi seluruh komponen perangkat keras jaringan dan perangkat lunak.

11.23 Pemfilteran Web.

11.23.1 Dept. TI memiliki daftar identifikasi jenis situs web yang boleh atau tidak boleh diakses dari jaringan TI Perusahaan.

11.23.2 Dept. TI melakukan blokir akses terhadap situs web yang memiliki jenis sebagai berikut:

a. Situs web yang memiliki fungsi unggah informasi kecuali diizinkan untuk alasan bisnis yang valid.
b. Situs web berbahaya yang diketahui atau dicurigai (mendistribusikan konten *malware* atau *phishing*).
c. Suatu *Command-and-Control* (C&C) *Server* yang memiliki sebuah *malicious network* yang dapat juga disebut sebagai *botnet*.
d. Situs web berbahaya yang diperoleh dari intelijen ancaman.
e. Situs web yang membagikan konten ilegal.

11.24 Penggunaan Kriptografi.

11.24.1 Untuk melindungi keutuhan informasi yang melewati jaringan umum, internet, harus digunakan teknik enkripsi yang memadai.

11.24.2 Dept. TI menetapkan standar kriptografi yang dipakai yaitu SSL 128 bit encryption.

11.24.3 Pengelolaan sertifikat digital (*digital certificate*), kunci kriptografi (*cryptographic keys*) dan parameter kriptografi terkait lainnya dilakukan oleh SDM Dept. TI yang ditetapkan dan dilindungi dari akses oleh pihak yang tidak berwenang.

11.24.4 Sistem dan teknik enkripsi hanya digunakan untuk melindungi informasi yang berisiko tinggi, dan penggunaannya harus mendapatkan izin dari VP Dept TI.

11.25 Siklus Hidup Pengembangan yang Aman.

11.25.1 Spesifikasi seluruh perangkat lunak yang dikembangkan baik oleh Dept. TI sendiri atau oleh mitra dan dimaksudkan untuk mengolah informasi yang penting, berharga atau rawan, harus didokumentasikan secara formal.

11.25.2 Spesifikasi sebagaimana dimaksud di atas harus disetujui baik oleh Pemilik sumber daya Teknologi informasi yang terlibat maupun oleh pengembang sistemnya sebelum kegiatan penulisan program dimulai.

11.25.3 Akses terhadap program *source library* harus dikendalikan secara ketat untuk mengurangi kemungkinan rusak, baik secara sengaja maupun tidak.

11.26 Persyaratan Keamanan Aplikasi.

11.26.1 Perangkat lunak *open source* diizinkan untuk digunakan di Perusahaan seperti halnya perangkat lunak komersial. Sebelum digunakan, baik perangkat lunak komersial maupun perangkat lunak *open source* harus dipastikan memenuhi persyaratan keamanan informasi yang berlaku.

11.27 Prinsip-prinsip Arsitektur dan Rekayasa Sistem yang Aman.

11.27.1 Koordinator Keamanan Teknologi informasi atau SDM yang ditugaskan, bertanggungjawab terhadap evaluasi pemenuhan persyaratan keamanan informasi oleh perangkat keras, perangkat lunak dan sistem lainnya yang akan digunakan.

11.28 Pengkodean yang Aman.

11.28.1 Dept. TI menetapkan perencanaan dan prasyarat sebelum pengkodean yang meliputi namun tidak terbatas pada:

a. Harapan spesifik-organisasi dan prinsip yang disetujui untuk pengkodean aman untuk digunakan baik dalam pengembangan kode internal dan yang dialihdayakan.
b. Praktik dan cacat pengkodean biasa dan historis yang mengarah pada kerentanan keamanan informasi.
c. Mengkonfigurasi alat pengembangan, seperti *integrated development environments* (IDE) untuk membantu melaksanakan pembuatan kode aman.

d. Mengikuti panduan yang dikeluarkan oleh penyedia alat pengembangan dan lingkungan eksekusi sebagaimana berlaku.
e. Pemeliharaan dan penggunaan alat pengembangan yang diperbarui.
f. Kualifikasi *Developer* dalam menulis kode yang aman.
g. Desain dan arsitektur yang aman, termasuk pemodelan ancaman.
h. Memiliki standar pengkodean yang aman dan jika relevan mewajibkan penggunaannya.
i. Penggunaan lingkungan yang terkendali untuk pengembangan.

11.28.2 Selama tahap pengkodean, perlu diperhatikan hal-hal sebagai berikut:
a. Praktik pengkodean yang aman spesifik untuk bahasa dan teknik pemrograman yang digunakan.
b. Menggunakan teknik pemrograman yang aman, seperti pemrograman berpasangan, *refactoring*, *peer review*, *security iteration* dan pengembangan berdasarkan pengujian.
c. Menggunakan teknik pemrograman terstruktur.
d. Mendokumentasikan kode dan memindahkan cacat pemrograman, yang dapat memungkinkan kerentanan keamanan informasi untuk dieksploitasi.
e. Melarang penggunaan teknik desain yang tidak aman (*hard-coded password, unapproved code samples* dan *unauthenticated web services*).

11.28.3 Pengujian dilakukan pada saat dan setelah tahap pengembangan, termasuk penggunaan *Static Application Security Testing* (SAST) dalam rangka mengidentifikasi kerentanan keamanan pada perangkat lunak.

11.28.4 Evaluasi keamanan kode program dilakukan terhadap:
a. *Attack surface* dan prinsip *Least Privilege*.
b. Melakukan analisis kegagalan pemrograman yang umum dilakukan dan mendokumentasikan mitigasi terhadap hal tersebut.

11.28.5 Pada tahap operasional terhadap aplikasi, dilakukan hal-hal sebagai berikut:
a. Pembaruan dikemas (*packaged*) dan *deployed* secara aman.
b. Penanganan terhadap kerentanan keamanan informasi yang dilaporkan.
c. Kesalahan (*errors*) dan dugaan serangan dicatat dan ditinjau secara reguler untuk penyesuaian kode jika diperlukan.
d. Kode sumber harus diproteksi dari akses dan gangguan yang tidak sah (*unauthorized*).

11.28.6 Penggunaan alat (tools) dan pustaka (*library*) eksternal mempertimbangkan:
a. Memastikan bahwa pustaka eksternal dikelola dengan baik (pemeliharaan inventaris pustaka yang digunakan dan versinya) dan secara reguler memperbarui dengan siklus rilis.
b. Seleksi, otorisasi, dan penggunaan kembali komponen yang telah diperiksa dengan

baik, khususnya komponen autentikasi dan kriptografi.

c. Lisensi, keamanan, dan riwayat komponen eksternal.

d. Memastikan bahwa perangkat lunak dapat dipelihara, dilacak dan berasal dari sumber yang telah terbukti dan memiliki reputasi.

e. Ketersediaan (*availability*) yang berjangka cukup panjang dari sumber daya dan artefak pengembangan.

11.28.7 Jika dibutuhkan modifikasi terhadap perangkat lunak, mempertimbangkan:

a. Risiko kendali bawaan dan proses integritas yang bobol.

b. Apakah akan mendapatkan persetujuan dari *vendor*.

c. Kemungkinan mendapatkan perubahan yang dipersyaratkan dari *vendor* sebagai pembaruan program standar.

d. Dampak jika organisasi menjadi bertanggung jawab atas pemeliharaan perangkat lunak di masa depan sebagai hasil dari perubahan.

e. Kompatibilitas dengan perangkat lunak lain yang digunakan.

11.29 Pengujian Keamanan dalam Pengembangan dan Penerimaan.

11.29.1 Dept. TI Perusahaan menetapkan kriteria uji terima (*acceptance criteria*) bagi sistem informasi baru, kriteria pemutakhiran (*upgrade*) atau kriteria versi baru sebelum digunakan di lingkungan kerja. Seluruh perubahan tersebut harus diuji sebelum diterima.

11.29.2 Secara formal, pelaksanaan penerimaan sistem diatur dalam Prosedur Pengembangan Aplikasi TI yang berlaku.

11.29.3 Kelemahan-kelemahan teknis sistem informasi yang digunakan harus segera diidentifikasi, dikaji risikonya, dan ditetapkan kendali-kendali untuk mencegah atau menutup kelemahan-kelemahan yang terjadi.

11.30 Pengembangan yang Dialihdayakan.

11.30.1 Setiap paket perangkat lunak yang dikembangkan oleh pihak eksternal baik mitra atau pihak eksternal lainnya, yang digunakan dalam sistem informasi milik Perusahaan, harus bebas dari mekanisme deaktivasi (pemberhentian operasi / layanan atau pentidakaktifan) yang dapat dipicu oleh mitra atau pihak eksternal lainnya tanpa sepengetahuan Dept. TI.

11.30.2 Dept. TI mengawasi dan memantau pengembangan perangkat lunak yang dilakukan oleh pihak mitra kerja untuk memastikan bahwa proses pengembangannya memenuhi syarat-syarat keamanan informasi yang ditetapkan dalam kontrak.

11.31 Pemisahan Lingkungan Pengembangan, Pengujian dan Produksi.

11.31.1 Untuk mengurangi peluang modifikasi aset informasi oleh pihak yang tidak berwenang atau peluang terjadinya kesalahan dalam penggunaan sistem informasi, atau untuk menghindari penyalahgunaan akses atau terjadinya perubahan sistem yang tidak dikehendaki, maka

harus dilakukan pemisahan fasilitas pengembangan, pengujian, dan operasional.

11.32 Manajemen Perubahan.

11.32.1 Dept. TI menetapkan prosedur pengendalian perubahan untuk mengelola perubahan pada aplikasi dan sistem operasi.

11.32.2 Jika sistem operasi berubah, maka aplikasi harus dievaluasi dan diuji lagi untuk menjamin bahwa keutuhan sistemnya tidak terganggu.

11.32.3 Dept. TI akan mengatur waktu pelaksanaan perubahan-perubahan terhadap sistem operasi dengan melibatkan para Pemilik Sumber Daya TI dan menyediakan waktu yang memadai untuk pengujian (*testing*).

11.32.4 Perubahan-perubahan terhadap perangkat lunak yang diperoleh dari Pihak Eksternal akan dikelola berdasarkan kontrak perjanjian dengan Pihak Eksternal tersebut.

11.33 Informasi Uji.

11.33.1 Data yang digunakan dalam pengujian sistem (*system test data*) harus dilindungi dari kemungkinan rusak, hilang, atau perubahan yang dilakukan tanpa izin.

11.34 Proteksi Sistem Informasi selama Pengujian Audit.

11.34.1 Menerapkan prosedur kendali akses yang sama untuk lingkungan uji seperti yang diterapkan untuk lingkungan operasional.

11.34.2 Memiliki otorisasi terpisah setiap kali informasi operasional disalin ke lingkungan uji.

11.34.3 Membuat *log* penyalinan dan penggunaan informasi operasional untuk menyediakan jejak audit.

11.34.4 Memproteksi informasi sensitif dengan pemindahan atau menyamarkannya jika digunakan untuk pengujian.

11.34.5 Menghapus secara layak informasi operasional dari lingkungan uji segera setelah pengujian selesai untuk mencegah penggunaan informasi uji yang tidak terotorisasi.

12. ALUR PROSES

- Tidak ada

13. LAMPIRAN

- Tidak ada