Kebijakan Keamanan Informasi

2022

Versi	1.2
Status	Final
Nomor Dokumen	C.Tel.002/HK 200/JDMT-1061400/2022
Tanggal	31-01-2022

PERATURAN DIREKSI

PT DAYAMITRA TELEKOMUNIKASI Tbk

NOMOR : C.Tel.002/HK 200/JDMT-1061400/2022

TENTANG

KEBIJAKAN KEAMANAN INFORMASI

Memimbang :

1. Bahwa sesuai dengan perkembangan teknologi dan kebutuhan organisasi aktivitas berbasis elektronik atau digital terutama dengan diterapkannya amanat Undang -Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ("UU ITE") melalui Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaran Sistem dan Transaksi Elektronik (**"PP PSTE"**), sehingga kewajiban bagi Perusahaan untuk mematuhinya menjadi efektif berlaku sesuai dengan ketentuan di dalam PP PSTE tersebut;
2. Kendali keamanan berbasis SNI atau Sistem Management Keamanan Informasi ISO 27001:2013.
3. Bahwa setiap penyelenggaraan Teknologi lnformasi (Tl) wajib memiliki aturan internal terkait kebijakan Keamanan Informasi Perusahaan;

Mengingat :

1. Anggaran Dasar PT Dayamitra Telekomunikasi sebagaimana tercantum dalam Akta Notaris H.M. Afdal Gazali,S.H. No.50, tanggal 18 Oktober 1995, dan telah disahkan oleh Menteri Kehakiman dan Hak Asasi Manusia dengan surat keputusan nomor C2-13273-HT.01.01.TH95 tanggal 19 Oktober 1995, anggaran dasar tersebut telah mengalami beberapa kali perubahan, perubahan terakhir sebagaimana tertuang dalam Akta Nomor 31 tanggal 21 Agustus 2021, yang dibuat dihadapan Notaris Fathiah Helmi, S.H., Notaris di Jakarta, yang telah diterima dan dicatat oleh Kementerian Hukum dan Hak Asasi Manusia RI melalui Keputusan Menteri Hukum dan HAM RI No. AHU-0045337.AH.01.02.TAHUN 2021 tanggal 23 Agustus 2021 tentang Persetujuan Perubahan Anggaran Dasar Perseroan Terbatas PT Dayamitra Telekomunikasi Tbk dan surat No. AHU-AH.01.03-0439750 tanggal 23 Agustus 2021 tentang Penerimaan Pemberitahuan Perubahan Anggaran Dasar PT Dayamitra Telekomunikasi Tbk dan Akta Nomor 5 tanggal 04 Januari 2022 yang dibuat dihadapan Notaris Fathiah Helmi, S.H., Notaris Jakarta, yang telah diterima dan dicatat oleh Kementerian Hukum dan Hak Asasi Manusia RI melalui Keputusan Menteri Hukum dan Hak Asasi Manusia RI melalui Keputusan Menteri Hukum dan HAM RI No. AHU-AH.01.03-0026982 tanggal 13 Januari 2022, mengenai perubahan Peningkatan Modal Ditempatkan/disetor pada PT Dayamitra Telekomunikasi Tbk.;
2. Akta Pernyataan Keputusan Pemegang Saham PT Dayamitra Telekomunikasi Nomor 01 tanggal 03 November 2020, dibuat oleh Tanti Lena, S.H.,M.Kn., Notaris dari Kota Tanggerang Selatan yang telah

diterima dan dicatat oleh Kemeterian Hukum dan Hak Asasi Manusia Republik Indonesia atas Pemberitahuan Perubahan Data Perseroan Nomor : AHU-AH-01.03-0403740 tanggal 30 November 2020.

MEMUTUSKAN :

Menetapkan : PERATURAN DIREKSI PT DAYAMITRA TELEKOMUNIKASI Tbk TENTANG KEBIJAKAN KEAMANAN INFORMASI.

BAB I
Pendahuluan

Pasal 1
Pengertian

Bahwa dalam Peraturan Direksi PT Dayamitra Telekomunikasi Tentang Kebijakan Keamanan Informasi (selanjutnya disebut "**Peraturan**") ini yang dimaksud dengan :

(1) **Aset Informasi** adalah seluruh aset Perusahaan yang berkaitan dengan kegiatan bisnis dan memiliki nilai finansial dalam bentuk data atau pengetahuan yang meliputi :

a. Aset *intangible*, berupa reputasi dan citra Perusahaan.

b. Aset Layanan: Layanan komputasi, komunikasi, dan sarana penunjang.

c. Aset infrastruktur informasi: *hardware* dan *software* yang digunakan untuk mengolah dan mengakses informasi Perusahaan.

d. Aset sumber daya manusia antara lain: Karyawan, keahlian dan pengalaman.

e. Aset dokumen dalam bentuk fisik atau digital.

(2) ***Availability*** adalah jaminan ketersediaan data atau informasi saat diakses dan digunakan oleh pihak yang sah.

(3) ***Confidentiality*** adalah jaminan kerahasiaan data atau informasi serta memastikan bahwa tidak tersedia atau diungkapkan kepada individu atau Proses yang tidak sah.

(4) **Direksi** adalah Direksi PT Dayamitra Telekomunikasi Tbk.

(5) **Enkripsi** adalah suatu metode yang digunakan untuk mengkodekan data sedemikian rupa sehingga keamanan informasinya terjaga dan tidak dapat dibaca tanpa didekripsi (kebalikan dari Proses enkripsi) dahulu.

(6) ***Firewall*** adalah suatu keamanan yang bersifat seperti sebuah filter yang bertujuan untuk menjaga (*prevent*) agar akses (ke dalam atau ke luar) dari orang yang tidak berwenang tidak dapat dilakukan.

(7) **Hak Akses Khusus** adalah pemberian hak akses untuk keperluan pemeliharaan dan pengujian sistem, serta audit.

(8) **Informasi Otentikasi Rahasia** adalah Informasi Rahasia yang digunakan untuk mengotentikasikan seorang Pengguna pada saat akan mengakses sebuah sistem informasi. Contoh dari informasi ini mencakup namun tidak terbatas pada *password, smartcard*, token, atau PIN.

(9) **Informasi Rahasia** adalah segala informasi yang diperoleh dari atau berkaitan dengan pelaksanaan Penggunaan TI Perusahaan sebagai Informasi Rahasia yang tidak dapat diungkapkan kepada pihak ketiga tanpa memperoleh persetujuan tertulis terlebih dahulu dari pihak yang memberikan informasi tersebut.

(10) **Informasi Vital** adalah informasi penting yang terekam untuk kelangsungan dan penyusunan kembali suatu organisasi. Hasil dari rekaman yang telah dicatat tersebut penting untuk menentukan kedudukan organisasi dimata hukum, seperti Udang-Undang atau peraturan dari suatu organisasi dan penting untuk dilindungi hak-hak suatu organisasi yang meliputi; para pegawai, pelanggan dan para pemegang saham.

(11) **Karyawan** adalah Karyawan Tetap dan atau Karyawan Kontrak atau orang yang bekerja pada Perusahaan dan menerima gaji berdasarkan hubungan kerja.

(12) **Keamanan Informasi (*Information Security*)** adalah aktifitas, proses, dan atau sistem yang bertujuan untuk menjaga serta mengamankan *Confidentiality*, integrity dan *Availability* dari informasi Perusahaan.

(13) **Kontrol** adalah aktifitas, proses, kebijakan, perangkat, latihan, atau aksi lainnya yang dapat mengendalikan/memodifikasi/mengurangi dan atau menghilangkan Risiko.

(14) **Kriptografi** adalah teknik-teknik matematika yang digunakan untuk menjaga Keamanan Informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta otentikasi data.

(15) **Layanan** adalah memberikan manfaat (*value*) kepada Pengguna dengan memfasilitasi hasil-hasil (*outcomes*) yang ingin dicapai Pengguna tanpa harus menanggung biaya-biaya dan risiko-resiko spesifik.

(16) ***Malware*** adalah istilah yang digunakan untuk perangkat lunak berbahaya yang dirancang untuk merusak atau melakukan tindakan yang tidak diinginkan terhadap sistem komputer, meliputi: virus, worm, trojan, spyware, dan perangkat lunak keamanan berbahaya lainnya.

(17) **Manajemen** adalah Direksi dan pimpinan dari unit kerja tertentu di Mitratel yang memiliki kewenangan manajerial dan terlibat dalam pengelolaan keamanan informasi.

(18) **Media Penyimpanan atau *Backup*** adalah seluruh media yang digunakan untuk menyimpan data dan atau informasi berbentuk elektronis.

(19) **Pengguna (*user*)** adalah individu akhir yang memiliki hak akses dalam suatu unit organisasi Perusahaan yang menggunakan Layanan sistem informasi.

(20) **Perangkat *Mobile*** adalah perangkat komputasi berukuran relatif kecil dan mudah di bawa-bawa.

(21) ***Privilege*** adalah hak akses yang diberikan kepada Karyawan dengan kemampuan dapat merubah sistem baik sebagian maupun keseluruhan sistem.

(22) **Prosedur** adalah suatu rangkaian aktivitas, tugas-tugas, tahapan, keputusan, perhitungan dan Proses yang bila dilakukan untuk memberikan hasil atau tujuan yang direncanakan.

(23) **Proses** adalah suatu aktivitas yang terstruktur.

(24) **Perusahaan atau Mitratel** adalah PT Dayamitra Telekomunikasi Tbk, termasuk anak Perusahaannya.

(25) **Risiko** adalah segala kejadian dalam setiap aktivitas Perusahaan yang timbul kerena faktor eksternal maupun internal, yang mengandung potensi menghambat pencapaian tujuan Perusahaan.

(26) ***Risk assessment* atau Penilaian Risiko** adalah metode yang sistematis untuk menentukan apakah suatu organisasi memiliki Risiko yang dapat diterima atau tidak.

(27) **Teknologi Informasi (TI)** adalah teknologi yang melibatkan pengembangan, pengelolaan, dan penggunaan semua sistem aplikasi yang mendukung Proses bisnis Perusahaan.

(28) **Unit Kerja** adalah kumpulan orang-orang yang bergabung dalam suatu kelompok, regu atau tim yang saling bekerjasama untuk menyelesaikan suatu pekerjaan.

Pasal 2
Sasaran

Sasaran utama dari Peraturan ini adalah memberikan arahan mengenai proses-proses Keamanan Informasi terkait dengan perlindungan terhadap aset TI yang digunakan. Keamanan Informasi dapat dicapai dengan penerapan secara menyeluruh dan konsisten terhadap Kontrol Keamanan Informasi yang tertuang dalam Peraturan ini. Penggunaan, dan pengelolaan informasi melatarbelakangi disusunnya Peraturan yang mengacu pada standar internasional sebagai panduan dalam penerapan Sistem Manajemen Pengamanan Informasi ("**SMPI**") di lingkungan Perusahaan.

Pasal 3
Tujuan

Tujuan ditetapkan Peraturan ini adalah untuk :

a. menyediakan kerangka kerja dalam penerapan pengendalian pengamanan informasi dan untuk meningkatkan pengertian umum mengenai SMPI yang disesuaikan dengan standar yang berlaku mengenai Keamanan Informasi.

b. Dengan adanya SMPI yang diterapkan di Mitratel diharapkan dapat meningkatkan perlindungan terhadap perangkat dan aplikasi dan mengurangi resiko penyalahgunaan informasi yang ada dalam rangka mengamankan data dan informasi milik Mitratel.

Pasal 4
Ruang Lingkup

Ruang Lingkup dalam Peraturan ini adalah pengelolaan, penggunaan, penyimpanan, pengolahan, pemusnahan dan pengiriman data sebagai salah satu bentuk Aset Informasi yang dimiliki oleh Mitratel dan berada di lingkungan Mitratel.

BAB II
Kebijakan Keamanan Informasi

Pasal 5
Fungsi Kebijakan Keamanan Informasi

Untuk melindungi Aset Informasi yang dikelola dan digunakan agar terhindar dari berbagai ancaman internal maupun eksternal yang meliputi keamanan data dan privasi, perangkat teknologi, infrastruktur dan sistem, seluruh aktivitas serta Proses yang terkait dengan penyediaan informasi.

(1) Kebijakan Keamanan Informasi

Aturan Kebijakan :

a. Dokumen Peraturan ini harus disetujui oleh Direksi Mitratel untuk penerapan di lingkungan Mitratel;

b. Dokumen Peraturan ini harus disosialisasikan kepada seluruh Karyawan Mitratel dan pihak eksternal.

(2) Peninjauan (*review*) Kebijakan Keamanan Informasi

Aturan Kebijakan :

a. Dokumen Peraturan ini harus dievaluasi setidaknya 1 kali dalam 1 tahun atau jika terdapat perubahan signifikan pada Proses dan TI untuk menjaga kesesuaian efektifitas penerapannya.

b. Apabila dari hasil peninjauan terdapat perubahan maka harus dilakukan pengkinian terhadap Peraturan.

BAB III
Organisasi Keamanan Informasi

Pasal 6
Organisasi Internal

(1) Manajemen Mitratel harus secara jelas menetapkan tugas dan tanggung jawab serta Proses koordinasi dalam Proses Keamanan Informasi.

(2) Sebuah struktur organisasi formal untuk mengelola SMPI di Mitratel.

(3) Struktur organisasi dapat bersifat struktural maupun fungsional. Struktur organisasi ini harus menjabarkan tugas dan tanggung jawab serta Proses koordinasi secara formal untuk pengelolaan SMPI dan peninjauan (*review*) terhadap implementasi SMPI dan Keamanan Informasi di Mitratel.

(4) Struktur organisasi SMPI harus diformalisasikan oleh pihak *top Management* SMPI di perusahaan melalui keputusan formal.

a. Tugas dan Tanggung Jawab Keamanan Informasi

Aturan Kebijakan :

1. Setiap Karyawan Mitratel harus memahami mengenai tanggung jawab terkait Proses yang dilakukan dan Keamanan Informasi yang diterapkan di lingkungan Mitratel untuk melindungi Aset Informasi yang digunakan.

2. Penetapan serta pengalokasian tugas dan tanggung jawab dalam pengelolaan SMPI dan Keamanan Informasi di Mitratel perlu dilakukan dengan jelas dan sesuai dengan kebutuhan SMPI dan Keamanan Informasi di Mitratel.

b. Pemisahan Tugas dan Tanggung Jawab

Aturan Kebijakan :

1. Tugas dan tanggung jawab dalam pekerjaan kritikal perlu dipisahkan untuk mengurangi Risiko adanya unsur ketidaksengajaan dalam penyalahgunaan Aset Informasi jaringan sesuai dengan Proses otorisasinya.
2. Hal ini dapat dilakukan dengan memastikan bahwa tidak ada seorangpun yang memiliki kemampuan untuk memodifikasi dan menggunakan Aset Informasi tanpa otorisasi atau deteksi.
3. Apabila pemisahan tugas dan tanggung jawab sulit untuk dilakukan, Kontrol tambahan perlu dipertimbangkan. Hal ini mencakup namun tidak terbatas pada pengawasan Manajemen dan/atau Audit Internal.
4. Proses audit SMPI dan Keamanan Informasi merupakan suatu Proses yang harus memiliki pemisahan tugas dan tanggung jawab yang jelas dimana seorang auditor tidak boleh mengaudit pekerjaannya sendiri.

c. Hubungan dengan pihak berwenang

Aturan Kebijakan :

1. Daftar nomor telepon pihak berwenang seperti pihak ketiga penyedia layanan jaringan, Polisi, Pemadam Kebakaran, Pihak Keamanan Gedung, dan lainnya perlu didata untuk menanggulangi gangguan terhadap Layanan tersebut.
2. Hubungan dengan pihak berwenang yang terkait dengan Keamanan Informasi perlu dipelihara.
3. Kontak tersebut perlu dilakukan apabila terjadi kejadian atau insiden yang perlu dilaporkan kepada pihak berwenang tersebut. Sebagai contoh, apabila terjadi pelanggaran hukum, maka kontak dengan pihak kepolisian perlu dilakukan.
4. Apabila perusahaan mengalami serangan melalui internet, maka pihak ketiga, seperti penyedia jasa layanan internet atau operator telekomunikasi perlu dihubungi untuk membantu mengatasi serangan tersebut.

d. Hubungan dengan Special Interest Group

Aturan Kebijakan :

1. Forum yang terkait dengan Keamanan Informasi atau asosiasi profesional Keamanan Informasi harus diikuti oleh personil admin *system* dengan tujuan untuk mengetahui informasi, yang terkait dengan Keamanan Informasi.
2. Hubungan tersebut perlu dilakukan dengan pertimbangan sebagai berikut :
   (a) Menambah pengetahuan mengenai *best practice* dan tetap mengikuti perkembangan teknologi dan informasi yang terkait dengan Keamanan Informasi.
   (b) Mendapatkan informasi akan kondisi Keamanan Informasi terkini.

(c) Mendapatkan informasi secara dini mengenai peringatan, informasi, saran, *update* atau *patch* yang terkait dengan Keamanan Informasi, dan

(d) Pertukaran informasi akan teknologi, produk, ancaman atau kerentanan terbaru yang terkait dengan Keamanan Informasi.

e. Keamanan Informasi Dalam Manajemen Proyek

Aturan Kebijakan :

1. Setiap pelaksanaan proyek di lingkungan Mitratel perlu diatur mengenai aspek Keamanan Informasi sebagai bagian dari perjanjian dan pelaksanaan proyek.
2. Mitratel harus melakukan *Risk Assessment* Keamanan Informasi pada fase awal pelaksanaan proyek untuk mengidentifikasi:
   (a) Risiko Keamanan Informasi yang relevan dalam pelaksanaan proyek
   (b) Kontrol Keamanan Informasi terkait dengan Risiko yang terindentifikasi.
3. Kontrol Keamanan Informasi yang telah teridentifikasi harus diimplementasikan selama proyek berlangsung, dan apabila diperlukan setelah proyek berlangsung.

Pasal 7
Identifikasi Infrastruktur Informasi Vital

(1) Identifikasi Infrastruktur Informasi Vital

Setiap sektor kritis bertanggung jawab untuk mengidentifikasi dan mengkategorikan infrastruktur Informasi Vital dalam infrastrukturnya berdasarkan Fungsionalitas, Skala Kekritisan, Tingkat Pelengkap Nilai Politik, Ekonomi, Sosial dan Strategis, tingkat ketergantungan, sensitivitas dan lain sebagainya.

Identifikasi infrastruktur kritis adalah Proses yang dinamis dan harus ditinjau secara berkala oleh semua pemangku kepentingan untuk mengatasi perubahan dependensi fungsional, teknologi, dan protokol. identifikasi infrastuktur informasi kritis merupakan bagian dari penilaian Risiko nasional yang merupakan pandangan holistik dari semua Risiko untuk keamanan nasional.

(2) Fungsionalitas

Fungsionalitas merupakan konsep dinamis yang mencakup seperangkat fungsi, Prosedur dan atau kemampuan yang terkait dengan sistem atau dengan bagian-bagian penyusunnya. Fungsionallitas dapat dilihat pada tingkat keunikan fungsional dan ketergantungan fungsional.

(3) Skala Kekritisan

Skala kekritisan berisi aturan heuristik untuk penilaian dampak berdasarkan pendekatan multidimensi yang mencakup ketersediaan, akses, penyampaian, dan penyempurnaan Layanan penting.

(4) Tingkat Komplementaritas

Aturan kebijakan:

a. Tingkat komplementaritas merupakan karakteristik yang membedakan dari infrastruktur informasi yang menghubungkan sistem infrastruktur informasi lainnya bersama-sama. Kegagalan satu sistem berpotensi mematikan infrastruktur Informasi Vital lainnya secara relatif cepat secara *cascading*.

b. Nilai politik, ekonomi, sosial, dan strategis mencakup apa yang dianggap penting bagi stabilitas politik, kemakmuran ekonomi, persaudaraan, persatuan, dan keutuhan Bangsa.

c. Durasi waktu memiliki arti penting dalam identifikasi dan kategorisasi infrastruktur Informasi Vital. Perbedaan waktu dan keaadaan dapat mempengaruhi tingkat kritis dari sistem yang sama.

Pasal 8
Unit Kerja Keamanan Informasi

(1) Unit Kerja Keamanan Informasi

Setiap organisasi harus merencanakan dan memiliki Unit Kerja Keamanan Informasi yang kuat dan independen. Unit Kerja ini harus bertanggung jawab untuk memastikan keselamatan dan keamanan Aset Informasi pada organisasi, sekaligus memastikan keselamatan dan keamanan data, Kontrol, dan segala sesuatu yang mengalir melalui infrastruktur Informasi Vital.

Unit Kerja Keamanan Informasi juga bertanggung jawab mencegah Informasi Rahasia atau kritis disebarluaskan dan memastikan penyebaran informasi yang relevan dan valid secara tepat waktu kepada elemen yang berwenang di setiap Infrastruktur Informasi Kritis yang teridentifikasi. Unit Kerja ini juga akan mempelajari ancaman, Risiko, kerentanan dan solusinya, memberikan pengarahan keamanan, mengamankan Informasi Rahasia, dan kegiatan pengajaran dan penegakan yang terkait dengan keamanan informasi.

Aturan kebijakan :

a. Infrastruktur Informasi Vital harus memiliki sistem Kontrol sendiri, sebagai contoh perangkat Kontrol Pengawasan dan Akuisisi Data yang dapat digunakan oleh spesialis khusus yang terpisah. Hal ini merupakan tanggung jawab Manajemen Senior untuk memastikan bahwa Unit Kerja-Unit Kerja tersebut memberikan masukan yang diperlukan ke Unit Kerja Keamanan Informasi di setiap tahap untuk memastikan perlindungan jaringan perusahaan yang berkelanjutan dan komprehensif.

b. Insiden keamanan, pelanggaran dan sejenisnya juga harus dilaporkan ke Unit Kerja Keamanan Informasi sesuai dengan kebijakan Keamanan Informasi organisasi.

c. Untuk mengelola domain infrastruktur Informasi Kristis yang beragam, diusulkan agar setiap organisasi dalam sektor kritis harus menunjuk *Chief Information Security Officer* (*CISO*), yang akan memimpin Unit Kerja Keamanan Informasi untuk berinteraksi dengan Pusat Perlindungan Infrastruktur Informasi Vital Nasional.

(2) Peran dan Tanggung Jawab Unit Kerja Keamanan Informasi

Aturan kebijakan :

a. Perencanaan

1. Identifikasi rencana kerja tahunan untuk mencapai tujuan keamanan dan tujuan yang konsisten dengan rencana Perusahaan.
2. Menentukan ruang lingkup dan batasan program Keamanan Informasi dan strategi implementasinya. Jika relevan, revisi rencana yang ada untuk memastikan perubahan, teknologi baru, dll.
3. Memahami persyaratan hukum dan peraturan.
4. Estimasi kebutuhan anggaran dan logistik. Harus ada pengaturan keuangan tahunan yang memadai untuk perencanaan, pemeliharaan dan pengelolaan Keamanan Informasi.
5. Menetapkan kerangka kerja Manajemen Risiko setelah merencanakan SMPI di seluruh organisasi sesuai dengan standar ISO/IEC 27001 dan standar keamanan lain yang relevan dengan berkonsultasi dengan Pusat Perlindungan Infrastruktur Informasi Vital Nasional.

b. Pengembangan

1. Memimpin dalam pengembangan kebijakan, standar, pedoman, proses, dan Prosedur Keamanan Informasi.
2. Menetapkan Proses formal untuk membuat, mendokumentasikan, meninjau, memperbarui, dan menerapkan kebijakan keamanan.
3. Perancangan dan pengembangan kebijakan informasi dan klasifikasi aset.
4. Memimpin dan mengkoordinasikan pengembangan kebijakan, Prosedur, pedoman, dan Proses keamanan informasi spesifik organisasi dengan berkonsultasi dengan berbagai pemangku kepentingan termasuk Pusat Perlindungan Infrastruktur Informasi Vital Nasional.

c. Manajemen

1. Melakukan sosialisasi kebijakan, Prosedur dan pedoman Keamanan Informasi kepada semua pihak.
2. Melakukan Penilaian Risiko, mengelola insiden, dan menyediakan pelaporan internal dan eksternal, keterlibatan dalam pendidikan dan pelatihan kesadaran keamanan.
3. Melakukan Integrasi Proses Keamanan Informasi dengan Proses bisnis organisasi.
4. Melakukan evaluasi berkala dan peninjauan efektivitas kebijakan, Prosedur, standar, pedoman, dan Proses Keamanan Informasi.
5. Memelihara catatan insiden dan pelanggaran Keamanan Informasi.
6. Mengkoordinasikan dan memimpin dalam implementasi 'rencana keberlangsungan bisnis dan melakukan pelatihan sejenis untuk mengevaluasi implementasi kegiatan tersebut secara efektif.
7. Memastikan kebijakan Manajemen Sumber Daya Manusia (SDM) secara memadai telah memasukkan Pedoman Keamanan Informasi, termasuk strategi Manajemen terkait Keamanan Informasi.

8. Memastikan penghapusan sistem secara aman.
9. Memastikan bahwa semua sistem informasi dalam organisasi dilengkapi dan diperbarui secara memadai.
10. Berinteraksi secara teratur dengan Unit Kerja yang mengelola fungsi TI pada untuk tetap mengikuti perkembangan teknologi / peralatan baru.

d. Pengawasan

1. Mengevaluasi efektivitas Proses operasional keamanan yang sedang berlangsung, memantau kepatuhan untuk persyaratan internal dan eksternal.
2. Mengevaluasi kepatuhan terhadap hukum dan peraturan persyaratan untuk Keamanan Informasi.
3. Melakukan audit Keamanan Informasi setidaknya setiap tahun atau setiap kali terjadi perubahan signifikan dalam sistem/infrastruktur IT. Unit Kerja Keamanan Informasi harus melaksanakan fungsinya setiap saat.

Pasal 9
Struktur Unit Kerja Keamanan Informasi

Aturan Kebijakan :

(1) Struktur Unit Kerja Kemanan Informasi harus hierarkis dengan *CISO* yang melapor langsung kepada kepala infrastruktur Informasi Vital /organisasi untuk memastikan pemahaman dan keterlibatan Manajemen Senior.

(2) *CISO* dapat dibantu oleh Unit Kerja yang berbeda dalam merancang Kebijakan Keamanan Informasi dan memastikan implementasinya yang efisien dan efektif.

(3) *CISO* dapat dibantu oleh dua Unit Kerja:

a. Pelatihan SDM dan Kebijakan bertanggung jawab atas tenaga kerja dan pelatihan yang dilakukan. Unit Kerja ini juga akan membantu dalam merancang kebijakan sistem informasi khusus untuk infrastruktur Informasi Kritis dengan berkoordinasi dengan Unit Kerja lain.

b. *Security Operation Center (SOC) and Incident Handling Response* yang bertanggung jawab atas Manajemen insiden Keamanan Informasi dan memberikan umpan balik untuk perbaikan sistem.

c. Selain hal di atas, dibutuhkan tim audit/ *pentest* untuk melakukan audit berkala sesuai kebijakan sistem informasi. Untuk menghindari potensi konflik kepentingan antara penegakan keamanan dan peran Manajemen *CISO* maupun peran audit dan pelaporan, Unit Kerja ini akan berada di luar kendali langsung *CISO* dan harus melapor langsung ke Manajemen senior organisasi.

BAB IV
Pengelolaan Aset

Pasal 10
Tanggung Jawab Terkait Aset

Untuk menjamin dan menjaga perlindungan terhadap Aset Informasi pada jaringan Mitratel, maka setiap Aset Informasi harus diidentifikasi serta ditentukan kepemilikan dari Aset Informasi tersebut.

(1) Inventarisasi Aset

Aturan Kebijakan :

a. Semua Aset Informasi yang digunakan di lingkungan data Center Mitratel harus didentifikasikan, diinventarisasi yang meliputi :

1. Informasi, yang dikelola di Mitratel.
2. Perangkat lunak dan aplikasi.
3. Aset fisik yang meliputi PC, Notebook, server, *removable media*, printer, dan scanner, mesin fotokopi dan lainnya.
4. Perangkat jaringan, Layanan jaringan, dan keamanan jaringan.
5. Sarana maupun Layanan pendukung seperti, Genset, UPS, dan AC, dan
6. Sumber daya manusia.

b. Daftar inventarisasi Aset Informasi tersebut harus diperiksa kesesuaian dan dilakukan pengkinian setiap ada perubahan yang terjadi.

c. Metode maupun tingkat pengamanan terhadap aset tersebut perlu ditentukan berdasarkan klasifikasi dari aset tersebut.

(2) Kepemilikan Aset

Aturan Kebijakan :

a. Setiap Aset Informasi yang digunakan di lingkungan Mitratel harus ditentukan penanggung jawab sebagai bagian pengelolaan aset tersebut, untuk:

1. Memastikan informasi dan Aset Informasi telah diklasifikasikan dan diamankan dengan baik.
2. Menentukan hak akses ke aset tersebut.
3. Secara periodik melakukan peninjauan terhadap klasifikasi dan pengamanan aset tersebut.

b. Pemeliharaan informasi atau aset dapat didelegasikan kepada pengelola (*custodian*) dari aset, namun tanggung jawab akhir dari informasi atau aset tersebut tetap terletak pada pemilik informasi atau aset tersebut.

(3) Penggunaan Aset Yang Diterima

Aturan Kebijakan :

a. Penggunaan perangkat TI hanya untuk kepentingan pekerjaan dan merupakan perangkat milik Mitratel.

b. Apabila ada penggunaan perangkat pribadi yang mengakses ke sistem Layanan jaringan Mitratel maka harus meminta persetujuan kepada pengelola Unit Kerja yang mengelola fungsi TI di Mitratel.

c. Akses ke Layanan jaringan dan komunikasi data bagi Karyawan Mitratel harus ditetapkan aturan dalam penggunaan Layanan tersebut untuk menghindari penyalahgunaan akses ke jaringan.

d. Aturan mengenai penggunaan informasi dan aset pemrosesan informasi harus dibuat, didokumentasikan dan diimplementasikan.

e. Semua Pengguna baik Karyawan Perusahaan maupun pihak ketiga harus mematuhi peraturan yang telah dibuat. Peraturan tersebut mencakup namun tidak terbatas pada:

   1. Aturan mengenai email dan penggunaan internet;

   2. Pedoman untuk penggunaan Perangkat *Mobile device*, khususnya penggunaan *device* di luar lingkungan kantor.

f. Seluruh Karyawan maupun pihak ketiga harus memiliki kesadaran (*awareness*) mengenai aturan penggunaan aset dan tanggung jawab Keamanan Informasi terkait dengan penggunaan aset tersebut.

(4) Pengembalian Aset

Aturan Kebijakan :

a. Setiap Karyawan yang sudah tidak berkerja di lingkungan Mitratel harus mengembalikan aset TI dan informasi milik Mitratel yang sudah bukan menjadi kewenangannya.

b. Aset yang dimaksud mencakup seluruh informasi dalam perangkat keras dan perangkat lunak.

c. Pengembalian aset TI dilakukan secara formal dan terdokumentasi sesuai dengan ketentuan yang berlaku.

Pasal 11
Klasifikasi Informasi

Untuk menjaga dan menjamin Keamanan Informasi, klasifikasi terhadap informasi perlu dilakukan dengan mempertimbangkan kebutuhan, prioritas, sensitifitas, dan kritikalitas dalam Proses bisnis Mitratel.

Klasifikasi tersebut perlu mempertimbangkan sensitifitas dan kritikalitas serta tingkat perlindungan yang diharapkan dalam penanganan informasi.

(1) Klasifikasi Informasi

Aturan Kebijakan :

a. Informasi harus diklasifikasikan sesuai dengan sensitifitas dan kritikalitas informasi tersebut bagi Perusahaan.

b. Klasifikasi informasi merupakan acuan untuk penanganan dan pengamanan informasi Perusahaan.

c. Pembagian tingkat klasifikasi dan penanganan informasi harus mempertimbangkan aspek kerahasiaan, integritas dan ketersediaan informasi.

d. Klasifikasi jenis Aset Informasi di Mitratel sesuai dengan kebutuhan dan dampak bisnis yang meliputi:

   1. Informasi Sangat Rahasia, yaitu informasi yang sangat sensitif dan hanya diperbolehkan untuk diakses pihak tertentu secara terbatas di lingkungan internal Mitratel;
   2. Informasi Rahasia, yaitu informasi yang sangat sensitif dan hanya dapat diakses oleh individu / pihak tertentu;
   3. Informasi Internal, yaitu data yang hanya dapat diakses oleh internal Mitratel;
   4. Informasi Umum, yaitu informasi yang dapat disebarkan ke publik.

e. Setiap pimpinan Unit Kerja di Mitratel dapat mengklasifikasikan Informasi Rahasia yang dianggap perlu diluar ketentuan perundang-undagan yang berlaku untuk mencegah kondisi yang menyebabkan gangguan terhadap Proses bisnis.

f. Klasifikasi informasi juga harus mempertimbangkan kebutuhan bisnis serta dampak terhadap bisnis apabila terjadi kegagalan keamanan.

g. Perlindungan terhadap Aset Informasi yang bersifat rahasia harus disesuaikan dengan tingkat keamanan yang memadai sesuai dengan klasifikasi informasi yang diterapkan di Mitratel.

h. Pemilik informasi bertanggung jawab untuk:

   1. Mengklasifikasikan informasi yang dimilikinya,
   2. Peninjauan secara periodik terhadap klasifikasi informasi untuk memastikan bahwa klasifikasi telah sesuai dengan kondisi dan kebutuhan terkini perusahaan (*up to date*).

(2) Pelabelan dan Penanganan Informasi

Aturan Kebijakan :

a. Prosedur terkait dengan pelabelan dan penanganan informasi harus dikembangkan dan diimplementasikan berdasarkan sistem klasifikasi informasi Perusahaan.

b. Penanganan informasi khususnya yang bersifat rahasia mencakup pada aspek pemrosesan, penyimpanan, distribusi, dan pemusnahan informasi harus diterapkan secara aman.

c. Prosedur pelabelan informasi harus mencakup segala bentuk informasi baik *hardcopy* maupun *softcopy*.

d. Informasi yang bersifat hardcopy harus diberi kodel (label) untuk memastikan penanganan informasi sesusai dengan tingkat klasifikasinya.

e. Data/informasi yang tersimpan dalam media elektronik (*softcopy*) harus

mendapatkan perlakukan sesuai kerahasiaannya dan diberikan password atau pembatasan akses ke *folder*.

(3) Prosedur penanganan informasi, yang mencakup Proses penyimpanan, transfer dan pemusnahan harus didefinisikan dengan jelas untuk setiap kategori klasifikasi.Penanganan Aset

Aturan Kebijakan :

a. Penanganan terhadap asset harus mengacu kepada keterkaitan dengan klasifikasi jenis Aset Informasi yang dikelola pada asset tersebut.

b. Prosedur penanganan aset diperlukan untuk melindungi informasi pada aset tersebut dari kegagalan terhadap aspek kerahasiaan, integritas dan ketersediaan.

c. Prosedur penanganan aset harus mencakup Proses, penyimpanan, dan pemindahan aset yang sesuai dengan klasifikasi informasi yang terdapat pada aset tersebut.

Pasal 12
Penanganan Media Penyimpanan Informasi

Pengelolaan ini diperlukan untuk mencegah pengungkapan (*disclosure*), modifikasi, *removal* atau penghancuran dari informasi yang tersimpan dalam media penyimpanan informasi sehingga harus dilindungi secara fisik.

(1) Pengelolaan *Removable* Media

Aturan Kebijakan :

a. Media yang digolongkan sebagai *removable media* antara lain adalah *tapes*, CD, DVD, *external hardisk*, USB *flash disk*, *memory card*.

b. *Removable media* yang digunakan dalam Mitratel perlu diregister, didokumentasikan apabila ada perubahannya, dan perangkat yang digunakan mempunyai fitur keamanan yang memadai.

c. Data yang terkandung dalam *removable media* yang tidak akan digunakan kembali harus dihapus secara permanen dan dipastikan tidak dapat di-*recover*.

d. Karyawan Mitratel harus selalu melakukan scanning virus terhadap *removable* media (flash disk, external harddisk) untuk mencegah adanya kerusakan informasi akibat *Malware*.

e. Semua *removable media* harus disimpan di tempat dan lingkungan yang aman.

f. *Removable media* yang tidak boleh digunakan untuk menyimpan informasi yang bersifat rahasia adalah CD, DVD, USB *flash disk*, dan *memory card*.

(2) Pemusnahan Media

Aturan Kebijakan :

a. Pemilik data/informasi atau pengelola media penyimpan data/informasi bertanggung jawab terhadap pemusnahan data/informasi.

b. Data/informasi yang dihapus dipastikan tidak dapat digunakan lagi, dibaca kembali,

atau diduplikasi ke media lain. Proses pemusnahan media dapat dilakukan dengan menggunakan mesin *shredding*.

c. Penghapusan informasi dari media penyimpanan elektronis dapat dilakukan dengan metode format ulang, penghancuran media, atau dengan metode *degaussing (*magnetisasi).

d. Dalam hal media penyimpan elektronis akan dialihkan peruntukkannya, maka data/informasi yang tersimpan dalam media tersebut yang dimaksud harus dihapus sebelum medianya dialihkan peruntukkannya.

e. Media penyimpanan informasi yang tidak digunakan kembali harus dimusnahkan dengan aman mengunakan Prosedur formal yang sudah ditetapkan. Hal ini perlu dilakukan untuk meminimalisasi Risiko kebocoran informasi milik Perusahaan.

f. Apabila pemusnahan media dilakukan oleh pihak ketiga, maka Kontrol yang memadai terhadap pihak ketiga tersebut harus diimplementasikan.

(3) *Physical* Media Transfer

a. Media yang menyimpan informasi milik Perusahaan harus dilindungi dari akses tanpa ijin, modifikasi dan penyalahgunaan selama dalam Proses pemindahan atau transportasi keluar dari area Perusahaan.

b. Beberapa hal berikut harus dipertimbangkan untuk melindungi Proses pemindahan media penyimpanan informasi.

1. Penggunaan media transportasi atau kurir yang terpercaya dan memiliki tingkat keandalan tinggi.

2. Pengemasan media harus dipastikan telah dilakukan dengan baik dan disesuaikan dengan jenis dan kondisi media untuk menghindari kerusakan fisik.

BAB V
Pengendalian Akses

Pasal 13
Prasyarat Bisnis Dalam Pengendalian Akses

Proses ini bertujuan untuk mengendalikan akses kepada seluruh Karyawan Mitratel dan pihak ketiga yang bekerja di lingkungan Mitratel untuk Keamanan Informasi Mitratel.

(1) Kebijakan pengendalian hak akses

Aturan Kebijakan :

a. Akses terhadap Informasi harus sesuai dengan kewenangan yang dimiliki dan *user id* yang *unique*.

b. Setiap Pengguna yang dapat mengakses sistem wajib menggunakan *user id* dan paswordnya masing-masing.

c. Standarisasi profil akses, sebagai contoh berupa hak akses administrator, dan Pengguna pada setiap sistem perlu ditetapkan.

d. Mekanisme untuk kegiatan pengajuan hak akses, otorisasi hak akses, pengadministrasian hak akses, pemantauan hak akses dilakukan secara periodik.

e. Kebijakan pengendalian akses ke informasi dan aset pemrosesan informasi (infrastruktur dan aplikasi TI) harus disusun, didokumentasikan, dan ditinjau sesuai kebutuhan.

f. Setiap pemilik informasi dan aset pemrosesan informasi bertanggung jawab untuk penyusunan kebijakan pengendalian hak akses tersebut.

g. Kebijakan tersebut dapat diwujudkan dengan penyusunan sebuah matriks hak akses untuk memetakan Pengguna dengan hak akses dan informasi atau aset pengolahan informasi.

h. Pengguna hanya akan diberikan akses ke informasi atau Aset Informasi Perusahaan berdasarkan kebutuhan operasional pekerjaannya.

(2) Akses ke Jaringan dan Layanan Jaringan

Aturan Kebijakan :

a. Fitur keamanan, tingkat Layanan dan kebutuhan terhadap Layanan jaringan yang diidentifikasi dalam operasional sistem di Mitratel harus dimonitor dan dievaluasi secara berkala.

b. Perangkat milik pribadi tidak diperkenankan terhubung ke jaringan internal Mitratel.

c. Semua akses ke perangkat Layanan jaringan MITRATEL hanya dapat dilakukan oleh pegawai penanggung jawab jaringan yang telah mendapatkan otorisasi dari pejabat yang mengelola fungsi IT di Mitratel.

d. Akses jaringan melalui *remote* harus mendapatkan persetujuan dari pejabat yang mengelola fungsi fungsi pada unit TI di Mitratel.

e. Penggunaan jaringan harus direview berkala melalui audit log yang dilakukan untuk mengidentifikasi kejadian atau kelemahan yang dapat menimbulkan kegagalan keamanan (*security breach*).

f. Fitur keamanan Layanan jaringan di Mitratel sedapat mungkin telah menerapkan teknologi pengamanan jaringan, seperti otentikasi dan Enkripsi jaringan.

g. Pengguna (*user*) hanya diperbolehkan untuk mengakses jaringan dan Layanan jaringan yang diijinkan sesuai area kerjanya.

h. Pemberian akses ke jaringan dan Layanan jaringan Perusahaan harus berdasarkan kebutuhan operasional pekerjaan Pengguna yang bersangkutan.

i. Perhatian lebih dan pengamanan tambahan harus diberikan untuk akses ke jaringan dan Layanan jaringan internal perusahaan dari jaringan internet (*remote access*).

Pasal 14
Pengelolaan Akses Pengguna

Proses ini bertujuan untuk memastikan Proses otorisasi user dan mencegah akses yang tidak memiliki otorisasi ke dalam sistem informasi yang mencakup semua tahapan mulai registrasi *account user* baru sampai dengan penghapusan *account* dari Pengguna yang tidak memerlukan lagi akses ke dalam sistem informasi.

Prosedur untuk mengelola hak akses user ke sistem informasi perusahaan harus ditetapkan.

(1) Pendaftaran Pengguna (*user*) dan penghapusan hak akses

Aturan Kebijakan :

a. Mitratel harus menerapkan Proses registrasi dan deregistrasi *user* untuk perijinan akses ke dalam sistem jaringan.

b. Pemberian hak akses Pengguna harus dilengkapi dengan otentikasi dan otorisasi serta harus diadministrasikan.

c. Penggunaan *user id* harus bersifat unik dan harus menunjukkan identitas nama dengan jelas bagi setiap Pengguna dan telah mendapatkan persetujuan dari Pimpinan Unit Kerja.

d. Memastikan bahwa tingkat hak akses yang diberikan kepada Pengguna telah sesuai dengan kewenangannya.

e. Segera mencabut atau menonaktifkan *user id* dan hak akses bagi Karayawan Mitratel yang telah berganti fungsi, tugas atau sudah tidak bekerja di Mitratel.

f. Menghindari penggunaan *user id* secara bersama (*shared*) kecuali untuk kondisi dimana penggunaan tersebut memiliki justifikasi operasional dan bisnis. Penggunaan *user id* harus disetujui secara formal dan didokumentasikan.

(2) Pemberian Hak Akses Pengguna

Aturan Kebijakan :

a. Pemberian hak akses Pengguna harus menerapkan Proses pengalihan atau pencabutan hak akses dari semua sistem dan Layanan.

b. Proses pengadaan untuk memberikan atau mencabut hak akses yang diberikan kepada *user id* meliputi :

   1. Memperoleh otorisasi dari Pejabat yang mengelola fungsi TI;
   2. Memverifikasi bahwa tingkat akses yang diberikan adalah sesuai dengan kebijakan akses;
   3. User yang telah rotasi/mutasi/ demosi/ promosi segera hak aksesnya di sesuaikan dengan posisinya;
   4. User yang telah pensiun segera hak aksesnya di hapus atau di blokir;
   5. Melakukan review pemberian hak akses secara berkala.

c. Permintaan hak akses harus diajukan secara formal oleh atasan langsung dari pemohon hak akses dan disetujui oleh pemilik dan administrator yang berwenang untuk sistem tersebut.

d. Persetujuan pemberian hak akses perlu memperhatikan kebutuhan operasional pekerjaan.

e. Pemberian hak akses harus di-*review* secara berkala untuk mengidentifikasi perubahan terhadap Pengguna seperti promosi, demosi, perpindahan posisi atau terminasi kepegawaian.

f. Seluruh Proses pemberian dari hak akses tersebut harus didokumentasikan dengan

baik.

(3) Hak Akses Khusus

Aturan Kebijakan :

a. Pemberian dan penggunaan Hak Akses Khusus untuk informasi (*read & write*) dan sistem informasi (*root, administrator*) Perusahaan harus dibatasi dan dikendalikan.

b. Proses otorisasi dan catatan dari semua Hak Akses Khusus yang diberikan harus didokumentasikan.

c. Hak Akses Khusus harus diberikan dalam format *user id* yang berbeda dengan hak akses biasa dan bersifat sementara.

d. Penggunaan Hak Akses Khusus harus dimonitor untuk memastikan tidak adanya akses tanpa ijin. Hak akses dengan tujuan untuk pelaksanaan audit terhadap sistem harus diberikan dengan wewenang read only.

e. Pengelolaan Hak Akses Khusus perlu memperhatikan beberapa hal berikut:

1. Persetujuan formal untuk Hak Akses Khusus perlu diberikan oleh pemilik dari informasi atau sistem informasi terkait.
2. Pemantauan / peninjauan secara berkala untuk Hak Akses Khusus yang telah dialokasikan.
3. Hak Akses Khusus yang digunakan secara bersama (*shared*) harus dilakukan Kontrol untuk mencegah penyalahgunaan melalui antara lain: *dual custody* dari password, penggantian password secara berkala atau penggantian password segera setelah salah satu pemegang password berhenti atau mengalami mutasi.

(4) Pengolaan Informasi Otentikasi Rahasia Milik Pengguna

Aturan Kebijakan :

a. Semua Pengguna harus memiliki *user id* dan hanya untuk digunakan secara individu.

b. Penggunaan *user id* secara bersama (*shared*) harus dibatasi dan hanya untuk kondisi dimana perangkat atau sistem yang dijalankan tidak memungkinkan pemisahan *user id* namun dengan persetujuan secara formal harus dilakukan oleh pejabat yang mengleola fungsi TI.

c. Pemberian Informasi Otentikasi Rahasia harus dikendalikan melalui Proses pengelolaan formal.

d. Pengelolaan Informasi Otentikasi Rahasia perlu memastikan:

1. Pengguna (user) memahami tanggung jawabnya untuk menjaga keamanan dari Informasi Otentikasi Rahasia yang dimilikinya.
2. Untuk Informasi Otentikasi Rahasia dalam bentuk *password*, apabila Pengguna terpaksa memberikan *password* tersebut kepada pihak lain. Maka, Pengguna harus mengganti informasi tersebut pada kesempatan pertama.
3. Pengguna dilarang memberikan Informasi Otentikasi Rahasia miliknya kepada pihak lain.

4. *Password* sementara yang tidak mudah ditebak dapat diberikan kepada Pengguna untuk melakukan akses untuk pertama kali ke sistem informasi Perusahaan. Pengguna harus segera mengganti *password* sementara tersebut.
5. Penyimpanan Informasi Otentikasi Rahasia harus dilakukan secara aman dengan perlindungan yang tepat.
6. Informasi Otentikasi Rahasia yang bersifat *default* dari *vendor* harus diganti setelah dilakukan instalasi sistem atau perangkat lunak.

(5) Peninjauan Terhadap Hak Akses Pengguna

Aturan Kebijakan :

a. Administrator sistem di Unit Kerja yang mengelola fungsi TI harus melakukan peninjauan terhadap hak akses user secara berkala.
b. Peninjauan dilakukan secara reguler, sekali setiap 6 (enam) bulan dan setiap ada perubahan terhadap Pengguna.
c. Otorisasi untuk hak *Privilege* harus ditinjau secara reguler dengan jangka waktu setiap 3 (tiga) bulan.
d. Peninjauan ini merupakan tanggung jawab dari pemilik informasi dan/atau sistem informasi terkait.
e. Perubahan pada hak *Privilege* perlu didokumentasikan.

(6) Pencabutan atau Penyesuaian Hak Akses

Aturan Kebijakan :

a. Pencabutan atau penyesuaian hak akses dari Karyawan Mitratel harus dihapus atau diblok untuk menentukan apakah perlu untuk penghapusan hak akses setelah pemutusan hubungan kerja, atau disesuaikan jika ada perubahan.
b. Beberapa saat sebelum Proses pemberhentian atau pergantian status kepegawaian perlu dipertimbangkan untuk membatasi akses kepada informasi atau sistem informasi Perusahaan.

Pasal 15
Tanggung Jawab Pengguna (*user*)

Proses ini bertujuan untuk mencegah akses tanpa otorisasi dan pencurian informasi. Pengguna harus memiliki pemahaman mengenai penggunaan dan tanggung jawabnya dalam memelihara Proses pengendalian akses secara efektif. Khususnya dalam penggunaan *password* dan pengamanan Aset Informasi yang dikelolanya. Pengguna wajib memiliki akuntabilitas untuk menjaga Keamanan Informasi dan sistem informasi Perusahaan yang diketahuinya. Kebijakan yang terkait dengan *clear desk* dan *clear screen* harus diimplementasikan untuk mengurangi Risiko pencurian atau kerusakan dari Aset Informasi.

(1) Penggunaan Informasi Otentikasi Pengguna yang Bersifat Rahasia

Aturan Kebijakan :

a. Setiap Karyawan Mitratel wajib menggunakan *password* di perangkat yang digunakan dan menjaga kerahasiaan *password* dan menghindari menyimpan catatan *password*

di tempat terbuka.

b. Setiap Karyawan Mitratel wajib mengganti *password* apabila ada indikasi sistem dan *password* mengalami penyalahgunaan atau kebocoran.

c. Penggunaan *password* harus yang berkualitas yang meliputi:

   1. Panjang minimal karakter *password* pada sistem dan perangkat yang digunakan adalah 6 (enam);
   2. Menggunakan kombinasi huruf dan angka, sedapat mungkin menggunakan spesial karakter (seperti: !$%#*) kecuali apabila sistem atau aplikasi tidak memungkinkan.
   3. Untuk sistem yang tidak dimungkinkan mengikuti penggunaan *password* yang berkualitas harus mendapatkan persetujuan dari pajabat yang mengelola fungsi TI di Mitratel dengan mempertimbangkan kendala dan Risiko yang ada.

d. Password tidak boleh sama dengan *user id* dan tidak berdasar pada sesuatu yang mudah ditebak sebagai contoh: nama, nomor telepon, tanggal lahir, nama anggota keluarga, nama/identitas Perusahaan.

e. Mengganti *password* secara reguler selama 3 (tiga) bulan dengan menghindari menggunakan *password* yang sudah pernah digunakan.

f. Setiap Pengguna wajib menjaga kerahasiaan password dan tidak diperkenankan memberikan *password*-nya kepada orang lain dan atau menggunakan *password* milik orang lain.

g. Pengguna diwajibkan untuk mengikuti kebijakan dan Prosedur yang berlaku dalam pemilihan dan penggunaan informasi otentikasi rahasia.

h. Terkait dengan keamanan Informasi Otentikasi Rahasia Password pengguna sistem informasi perlu :

   1. Password tidak terdiri dari urutan karakter baik angka, huruf maupun lokasi pada keyboard, seperti 12345678, asdfgh atau 1234zxcv.
   2. Mengganti password sementara pada saat pertama kali log-on.
   3. Tidak menggunakan atau memasukkan password ke sistem secara otomatis.
   4. Tidak menggunakan password yang sama untuk penggunaan bisnis dan pribadi.
   5. Untuk penggunaan Informasi Rahasia yang bersifat password beberapa hal berikut harus dijalankan :
      (a) Menggunakan password yang mudah diingat, namun tidak mudah ditebak
      (b) Tidak terdiri dari urutan karakter baik angka, huruf maupun lokasi pada keyboard, seperti 12345678, asdfgh atau 1234zxcv.
      (c) Mengganti password sementara pada saat pertama kali log-on.
      (d) Tidak menampilakan karakter password pada saat log-on. Tampilan karakter password dapat diganti dengan simbol.

i. Administrator pengelola sistem informasi perlu memperhatikan dengan seksama dan

mencatat setiap laporan kehilangan Informasti Otentikasi Rahasia atau permintaan *password reset*.

(2) Pengendalian Akses Informasi dan Aplikasi

a. Proses ini bertujuan untuk mencegah akses tanpa wewenang ke sistem di Mitratel dengan membatasi akses ke sistem jaringan.

b. Pengendalian dilakukan dengan membatasi akses ke informasi dan sistem aplikasi Perusahaan.

(3) Pembatasan akses informasi

Aturan Kebijakan :

a. Akses ke informasi pada sistem jaringan oleh Pengguna harus dibatasi sesuai dengan kewenangan akses.

b. Pembatasan akses dilakukan berdasarkan kebutuhan Karyawan sesuai dengan keperluan operasional dan bisnis tersebut.

c. Pembatasan akses perlu dilakukan untuk informasi pada sistem informasi. Hal ini dapat dilakukan antara lain dengan pengendalian hak untuk *read, write, copy* maupun *delete.*

(4) Prosedur log-on secara aman

Aturan Kebijakan :

a. Akses ke sistem operasi harus dikontrol dengan menggunakan mekanisme *secure logon* meliputi :

1. Tidak memberikan pesan bantuan yang dapat menyebabkan *log-on* tanpa ijin.
2. Membatasi jumlah kesalahan dalam percobaan *log-on* serta melakukan hal-hal berikut apabila jumlah kesalahan maksimal telah terlewati maka hal tersebut perlu dipertimbangkan :
   (a) Merekam setiap percobaan *log-on* baik yang gagal maupun berhasil.
   (b) Memberikan jeda waktu sebelum *log-on* dapat dilakukan kembali atau menolak percobaan kembali setelah terjadi kesalahan dalam percobaan *log-on.*
   (c) Memutuskan koneksi data.
   (d) Memberikan pesan peringatan pada sistem bahwa jumlah maksimal percobaan *log-on* telah terlewati.
   (e) Jumlah maksimal percobaan *log-on* perlu mempertimbangkan panjang minimal dari *password* dan nilai dari sistem yang dilindungi.
3. Tidak menampilkan karakter password pada saat *log-on*. Tampilan karakter *password* dapat diganti dengan simbol.
4. Tidak memberikan petunjuk mengenai sistem atau aplikasi sebelum Proses *log-on* telah sukses dilakukan.

5. Menampilkan peringatan, bahwa sistem atau aplikasi hanya boleh diakses oleh orang yang berkepentingan.
6. Validasi informasi *log-on* hanya setelah seluruh data telah dimasukkan kedalam Proses *log-on*. Apabila terjadi kesalahan input data pada Proses *log-on* sistem tidak boleh mengindikasikan bagian data mana yang salah.
7. Membatasi waktu minimal dan maksimal untuk Proses *log-on*.
8. Setelah Proses *log-on* yang berhasil sistem perlu menampilkan waktu dari Proses *log-on* terakhir, baik yang berhasil maupun yang gagal.
9. Tidak mentransmisikan *password* dalam *clear text* melalui jaringan.

(5) Sistem Pengelolaan P*assword*

Aturan Kebijakan :

a. Sistem Manajemen password harus memastikan penggantian *password* secara reguler yaitu maksimal 3 (tiga) bulan sekali.
b. Sistem untuk mengelola *password* perlu menggunakan sistem yang interaktif dan harus dapat memastikan kualitas *password* Pengguna sistem informasi perusahaan.
c. Sistem Manajemen *password* harus memastikan :
    1. Penggunaan *user ID* dan *password* individual untuk setiap Karyawan.
    2. Pengguna dapat mengganti *password*-nya.
    3. Memastikan penggunaan *password* yang sesuai dengan aturan terkait penggunaan *password*.
    4. Memastikan Pengguna mengganti *password* sementara pada saat *log-on* untuk pertama kali.
    5. Tidak menampikan *password*.
    6. Menyimpan file yang berisi *password* secara terpisah dari data aplikasi.
    7. Penyimpanan dan pengiriman *password* harus menggunakan perlindungan khusus seperti Enkripsi dan *hashing.*

(6) Penggunaan Program utilisasi Khusus.

Aturan Kebijakan :

a. Penggunaan *system utility programs* yang berpotensi dapat mengambil alih pengendalian sistem jaringan harus dibatasi dan dikendalikan secara ketat.
b. Administrator Jaringan harus melakukan Proses identifikasi, otentikasi dan otorisasi untuk seluruh *system utilities* yang digunakan dan membatasi penggunaan *system utilities.*
c. Contoh dari *system utility* tersebut adalah aplikasi yang memiliki akses ke *registry* sistem operasi atau aplikasi yang memiliki akses langsung untuk memanipulasi *database.*
d. Penggunaan *system utility* harus diberikan hanya kepada Karyawan yang memiliki

kebutuhan operasional yang valid dan harus disetujui oleh pemilik dari sistem yang diaksesnya.

(7) Pengendalian akses ke *source code* program

a. Akses ke *source code* program beserta dokumentasi terkait lainnya seperti desain, spesifikasi, verifikasi dan validasi, harus dikendalikan secara ketat untuk mencegah akses tanpa ijin. Hal ini dapat dilakukan melalui penyimpanan *source code* secara terpusat.

b. Beberapa hal berikut dapat dipertimbangkan dalam pengendalian akses ke source code program :

(1) Penyimpanan *source code* tidak dilakukan pada sistem operasional.

(2) Prosedur pengendalian akses *source code* perlu disusun dan diimplementasikan

(3) Diperlukan Proses otorisasi resmi untuk mengakses *source code*.

(4) Daftar *source code* perlu dibuat, dipelihara dan dijaga.

(5) Setiap akses ke *source code* program perlu didokumentasikan, termasuk *audit log* untuk akses tersebut.

(6) Pemeliharaan dan penyalinan *source code* program harus dilakukan melalui mekanisme pengendalian perubahan.

Pasal 16
Pengendalian Alat Akses Jarak Jauh

Proses ini bertujuan untuk mencegah pencurian, akses tidak sah, atau perusakan Aset Informasi di Mitratel dengan membatasi penggunaan alat akses jarak jauh. Pengendalian dilakukan dengan menetapkan persyaratan untuk alat akses jarak jauh yang digunakan di Mitratel.

Aturan Kebijakan :

(1) Semua alat atau sistem akses jarak jauh yang memungkinkan komunikasi ke sumber daya Mitratel dari Internet atau sistem mitra eksternal harus memerlukan otentikasi multi-faktor. Sebagai Contoh termasuk token otentikasi dan *smart cards* yang memerlukan PIN atau kata sandi tambahan.

(2) Sumber database autentikasi harus berupa *active directory* atau *Lightweight Directory Access Protocol (LDAP),* dan protokol autentikasi harus melibatkan protokol *challenge-response* yang tidak rentan terhadap serangan replay. Alat akses jarak jauh harus saling mengotentikasi kedua ujung sesi.

(3) Alat akses jarak jauh harus mendukung proxy lapisan aplikasi Mitratel daripada koneksi langsung melalui perimeter Firewall.

(4) Alat akses jarak jauh harus mendukung Enkripsi ujung-ke-ujung yang kuat dari saluran komunikasi akses jarak jauh sebagaimana ditentukan dalam kebijakan protokol Enkripsi jaringan Mitratel.

(5) Semua antivirus Mitratel, pencegahan kehilangan data, dan sistem keamanan lainnya tidak boleh dinonaktifkan, diganggu, atau dielakkan dengan cara apa pun.

(6) Semua alat akses jarak jauh harus dibeli melalui Proses pengadaan yang berlaku di Mitratel,

dan Unit Kerja yang mengelola TI harus menyetujui pembelian tersebut.

Pasal 17
Kontrol Integrasi

Kontrol ini berkaitan dengan Sistem Kontrol industri yang berinteraksi dengan sistem keamanan *cyber*.

Aturan Kebijakan :

(1) Pentingnya Kontrol keamanan *cyber* telah diakui. Oleh karena itu, penting bagi setiap strategi perlindungan keamanan *cyber* untuk sektor (Infrastruktur Informasi Vital Nasional) oleh BSSN (Badan Siber dan Sandi Negara) untuk mempertimbangkan sistem/Proses yang ada yang sudah diterapkan oleh industri

(2) Kontrol ini bertujuan untuk memastikan bahwa semua sistem yang digunakan di Perusahaan Infrastruktur Informasi Vital Nasional diamankan secara memadai, dan secara sesuai menggabungkan prinsip pertahanan secara mendalam.

(3) Infrastruktur Informasi Vital harus memastikan bahwa semua jaringan interkoneksi dilindungi dengan benar, dengan perlindungan yang memadai dibangun di kedua sisi (untuk jaringan milik Perusahaan), atau, dengan perlindungan yang memadai dibangun untuk menahan penolakan / gangguan / kerusakan dari jaringan antarmuka.

(4) Analisis dampak kegagalan/gangguan, baik karena pemadaman sistem, atau, karena perubahan konfigurasi atau *commissioning*/penonaktifan peralatan/sistem baru atau yang diperbarui harus dipertimbangkan pada tahap perencanaan itu sendiri.

BAB VI
Kriptografi

Pasal 18
Pengendalian Kriptografi

Proses ini bertujuan untuk menjaga kerahasian, keaslian dan integritas informasi dengan menggunakan teknologi Kriptografi.

(1) Kebijakan penggunaan Kriptografi

Aturan Kebijakan :

a. Setiap sistem jaringan harus mempertimbangkan penggunaan Kriptografi yang mencakup tipe, kekuatan dan kualitas dari algoritma Kriptografi yang digunakan pada jaringan. Algoritma Kriptografi yang sudah terbukti dapat dipecahkan dengan mudah tidak boleh digunakan oleh organisasi.

b. Penggunaan teknologi Kriptografi dapat digunakan untuk melindungi informasi milik Mitratel.

c. Keputusan penggunaan teknologi Kriptografi perlu menimbang sensitifitas (sisi kerahasiaan) dan kritikalitas (sisi integritas) dari informasi yang akan dilindungi.

d. Penggunaan Enkripsi harus dipertimbangkan untuk melindungi informasi sensitif dan atau rahasia yang dipindahtangankan atau dikirimkan baik melalui media jaringan informasi maupun transportasi secara fisik menggunakan *removable media* atau

device.

e. Implementasi Kriptografi perlu mempertimbangkan aspek hukum dan regulasi negara, yang mungkin membatasi penggunaan Kriptografi terutama untuk pengiriman data antar negara.

(2) Manajemen dari *key* untuk kebutuhan Kriptografi

Aturan Kebijakan :

a. Seluruh *key* Kriptografi harus dilindungi dari modifikasi, kehilangan serta kerusakan.

b. Sistem manajemen dari *key* Kriptografi perlu berdasar pada mekanisme pengelolaan *key* yang memadai.

c. Peralatan yang digunakan untuk mengasilkan dan menyimpan *key* Kriptografi harus dilindungi secara fisik.

d. Pengelolaan dari *key* Kriptografi harus dikendalikan secara ketat dan dibatasi hanya pada Pengguna yang terotorisasi. Apabila memungkinkan, pengelolaan dari *key* Kriptografi didasarkan pada prinsip *dual custody* untuk mengurangi Risiko penyalahgunaan.

e. Apabila terdapat indikasi kebocoran *key* Kriptografi, maka *key* tersebut harus segera dicabut dan diganti.

f. Detail pengelolaan *key* Kriptografi dapat dilihat dari Prosedur Enkripsi dan manajemen Kunci Kriptografi.

BAB VII
Keamanan Sumber Daya Manusia

Pasal 19
Sebelum status kepegawaian dimulai (*Prior to employment*)

Proses keamanan sumber daya manusia dimulai sejak sebelum status kepegawaian dimulai. Status kepegawaian ini juga mencakup pihak ketiga yang memiliki aktivitas pekerjaan di lingkungan Mitratel.

(1) Penyaringan (*screening*)

Aturan Kebijakan :

a. Penyaringan terhadap calon Karyawan harus dilakukan sebagai bentuk pemeriksaan dan verifikasi terhadap informasi pribadi dan latar belakang dari calon Karyawan, yang mencakup namun tidak terbatas pada:

1. Referensi mengenai karakter pribadi, baik secara pribadi maupun profesional;
2. Verifikasi kelengkapan dan kebenaran CV pribadi;
3. Konfirmasi kebenaran kualifikasi akademik dan profesional;
4. Verifikasi identitas (KTP, Passport dan atau SIM);
5. Pemeriksaan catatan kriminal.

b. Hal ini harus dilakukan sesuai dengan peraturan perundang-undangan, regulasi dan

etika.

c. Proses penyaringan ini juga perlu menyesuaikan dengan kebutuhan bisnis, klasifikasi informasi dan Aset Informasi yang akan diakses oleh calon Pengguna tersebut serta Risiko yang ada.

d. Kriteria penilaian untuk Proses penyaringan ini perlu dibuat untuk menjamin Proses penyaringan yang berkelanjutan (*reproduceable* dan *repeatable*).

e. Informasi mengenai calon Pengguna informasi dan sistem informasi yang diperoleh pada Proses penyaringan harus dikumpulkan dan ditangani sesuai dengan aturan hukum perundang-undangan yang berlaku.

f. Proses ini diatur dalam Peraturan Direktur Keuangan No PR. 2040/HC2/DKA-10000000/XI/2019 Tentang Pola Rekrutasi Karyawan.

(2) Syarat dan Ketentuan Pegawai

Aturan Kebijakan :

a. Setiap Karyawan Mitratel dan pihak ketiga harus memahami tata tertib organisasi, hal ini untuk memastikan tanggung jawab terkait aktivitas pekerjaan di Mitratel.

b. Setiap Pengguna informasi maupun sistem informasi Perusahaan harus menyetujui dan menandatangani syarat dan ketentuan terkait dengan Keamanan Informasi dan sistem informasi Perusahaan.

c. Syarat dan ketentuan tersebut tercakup dalam Peraturan Direktur Keuangan Tentang Pola Rekrutasi Karyawan Mitratel.

Pasal 20
Pada saat status kepegawaian berjalan

Pengguna informasi dan sistem informasi Perusahaan harus memahami tugas dan tanggung jawab serta Risiko yang terkait dengan Keamanan Informasi selama status kepegawaiannya masih berjalan.

Hal ini bertujuan untuk memastikan keamanan operasional sistem manajemen Keamanan Informasi dan mengurangi Risiko kesalahan manusia (*human error*). Tingkat kesadaran (*awareness*) dan pelatihan mengenai Keamanan Informasi harus diberikan secara periodik bagi semua Pengguna informasi dan sistem informasi Perusahaan. Proses ini bertujuan untuk menjamin bahwa Karyawan Mitratel dan pihak ketiga yang bekerja di lingkungan Mitratel memahami ancaman yang terkait dengan keamanan data, informasi dan privasi termasuk tanggung jawabnya.

(1) Tanggung Jawab Manajemen

Aturan Kebijakan :

a. Semua pimpinan Unit Kerja di lingkungan Mitratel perlu memastikan bahwa Karyawan memahami kebijakan dan Prosedur kerja yang berlaku.

b. Semua pimpinan Unit Kerja di lingkungan Mitratel agar memastikan bahwa Pengguna informasi dan sistem informasi menerapkan Proses Keamanan Informasi sesuai dengan kebijakan dan prosedur yang berlaku.

c. Tanggung jawab Manajemen adalah untuk memastikan bahwa semua Pengguna informasi dan sistem informasi :

1. Telah memahami dan memiliki pedoman terkait dengan tugas dan tanggung jawabnya dalam sistem Keamanan Informasi Perusahaan.
2. Mematuhi seluruh tugas dan tanggung jawabnya sesuai dengan syarat dan ketentuan pada perjanjian kerjanya dan kebijakan Keamanan Informasi perusahaan.
3. Memiliki keahlian dan kualifikasi Keamanan Informasi sesuai dengan tugas dan tanggung jawabnya.

(2) Kesadaran, Pendidikan dan Pelatihan Terkait Dengan Keamanan Informasi .

Aturan Kebijakan :

a. Sosialisasi mengenai Keamanan Informasi kepada semua Karyawan Mitratel harus dilakukan secara berkala sesuai dengan tugas dan wewenang yang diberikan.

b. Pelatihan kesadaran tentang Keamanan Informasi Perusahaan harus dilakukan sebelum Pengguna diberikan akses terhadap informasi dan sistem informasi.

c. Pelatihan tersebut harus disesuaikan dengan pekerjaan, tanggung jawab dan pengendalian Keamanan Informasi bagi Karyawan.

(3) Proses Pendisiplinan

Aturan kebijakan :

a. Setiap Karyawan yang melakukan pelanggaran terkait Keamanan Informasi harus dilakukan Proses kedisplinan secara formal sesuai dengan tata tertib organisasi.

b. Pejabat yang mengelola fungsi Unit TI harus mempertimbangkan bentuk sanksi yang tegas sesuai dengan tingkat pelanggaran yang dilakukan.

c. Sanksi yang tegas seperti pemberhentian kerja atau pencabutan hak akses dapat diberlakukan sesuai dengan pelanggaran yang dilakukan dan Proses yang berlaku.

d. Proses kedisiplinan akan mengikuti Proses yang diatur dalam Peraturan Direktur Keuangan tentang Pola Rekrutrasi Karyawan.

Pasal 21
Pemberhentian atau pergantian status kepegawaian.

Proses ini dilakukan untuk menjamin Proses pemberhentian atau pergantian tugas dan fungsi Pengguna informasi atau sistem informasi berjalan dengan baik.

Tanggung jawab pengeloaan Proses ini perlu diberikan kepada Karyawan atau Unit Kerja tertentu untuk menjamin pengembalian informasi, Aset Informasi, dan hak akses telah dilakukan.

Proses ini perlu dilakukan secara transparan untuk menjamin tidak adanya kebocoran informasi karena ketidak tahuan dari Pengguna atau rekan Pengguna akan adanya Proses pemberhentian atau pergantian status kepegawaian.

Aturan Kebijakan :

(1) Setiap pimpinan Unit Kerja di Mitratel harus memperhatikan Proses terminasi atau mutasi terhadap Karyawan yang berada Mitratel sesuai dengan Prosedur yang berlaku.

(2) Tanggung jawab dalam Proses pemberhentian atau pergantian status kepegawaian perlu secara jelas didefinisikan dan dialokasikan kepada Unit kerja yang bersangkutan.

(3) Tanggung jawab Pengguna pada saat dan setelah Proses pemberhentian atau pergantian status kepegawaian harus dikomunikasikan dengan jelas kepada Karyawan yang bersangkutan.

Proses kedisiplinan akan mengikuti Proses yang diatur dalam Peraturan Mitratel mengenai Status dan Hubungan Kerja serta Pemutusan Hubungan Kerja.

Pasal 22
Keamanan Fisik dan Lingkungan

(1) Wilayah yang Aman

Wilayah yang aman diperoleh melalui pembatasan wilayah dengan menggunakan pembatasan fisik untuk mencegah akses fisik tanpa ijin yang dapat menimbulkan gangguan, kehilangan atau kerusakan terhadap Aset Informasi milik Mitratel. Area Perusaahaan dibagi menjadi 2 (dua), yaitu:

a. Area Terbatas

Area terbatas merupakan area yang dapat diakses oleh pihak yang berwenang, yaitu Karyawan, pihak ketiga yang memiliki hubungan pekerjaan dengan Perusahaan, serta pihak yang memiliki kepentingan bisnis maupun operasional dengan Perusahaan.

Area yang dikategorikan sebagai area terbatas dalam Perusahaan mencakup ruang kantor dengan ketentuan kendali perimeter,kebakaran, dan personel yang terdiri antara lain:

(1) Ruang kerja Karyawan;

(2) Ruang rapat;

(3) Area Perusahaan selain yang masuk dalam kategori area keamanan khusus.

b. Area Keamanan Khusus

Area keamanan khusus merupakan area yang didalamnya terdapat informasi dan fasilitas yang bersifat kritikal yang perlu dilindungi dari akses tanpa ijin, kerusakan dan gangguan.

Area yang dikategorikan sebagai keamanan khusus dalam Perusahaan mencakup:

a) Pusat Data yang mencakup ketentuan kendali perimeter, kelistrikan, lingkungan, kebakaran dan personel;

b) Area Tower yang mencakup ketentuan kendali perimeter, kebakaran, dan personel.

Detail terkait pengelolaan dan pengamanan fisik dan lingkungan untuk area Perusahaan diatur dalam dokumen Standar Keamanan Fisik.

(2) Perimeter Keamanan Fisik

Aturan Kebijakan :

a. Pembatasan wilayah dengan pembatas secara fisik harus digunakan untuk melindungi area yang berisi informasi dan atau fasilitas pengolahan informasi.

b. Pengamanan fisik ruangan di Mitratel mengacu kepada klasifikasi wilayah masing-masing ruangan dengan menggunakan pembatas dan pengendalian akses fisik (berupa: kartu Kontrol akses).

c. Akses ke dalam area Perusahaan harus dibatasi dengan antara lain membuat daerah penerimaan tamu yang dijaga atau melengkapi pintu dan jendela dengan kunci secara fisik maupun elektronik untuk menjamin akses hanya untuk Karyawan yang berkepentingan.

d. Akses ke dalam area Perusahaan harus di pantau untuk mendeteksi aktivitas yang dapat menimbulkan kerugian Perusahaan.

e. Fasilitas pemrosesan informasi harus diletakkan di dalam ruangan yang memiliki Kontrol pengamanan akses keluar masuk yang memadai.

f. Fasilitas pemrosesan informasi Perusahaan harus terpisah secara fisik dari area kerja pihak ketiga.

g. Pintu darurat perlu dilengkapi dengan alarm yang dimonitor dan diuji secara berkala untuk memastikan berfungsi sebagaimana mestinya.

(3) Pengendalian akses fisik

Aturan Kebijakan :

a. Akses fisik wilayah aman harus dikendalikan untuk menjamin tidak adanya akses tanpa ijin.

b. Tamu atau pihak ketiga yang datang ke area kerja di Mitratel dicatat tanggal dan waktu masuk maupun keluarnya, harus tetap didampingi atau diawasi kecuali telah mendapatkan ijin akses. Pengunjung perlu diberi informasi mengenai syarat keamanan area keamanan khusus beserta Prosedur dalam keadaan darurat.

c. Tamu atau pihak ketiga yang mengakses area kritikal di Mitratel hanya untuk Karyawan yang mempunyai kewenangannya dan diotorisasi oleh Pejabat penanggung jawab di ruang tersebut dan harus diawasi dan didampingi oleh Karyawan di ruangan tersebut.

d. Akses masuk ke dalam area tempat pemrosesan/penyimpanan informasi sensitif harus dikendalikan melalui penggunaan kartu akses atau PIN. *Audit trail* terkait akses ke dalam area tersebut harus dikelola dengan baik.

e. Semua Pengguna baik internal maupun eksternal wajib mengenakan *id card* ketika masuk ke dalam area Perusahaan. Pengguna harus segera melaporkan kepada petugas yang berwenang seandainya ditemukan Pengguna yang tidak mengenakan *id card.*

f. Hak akses ke area keamanan khusus harus selalu ditinjau secara rutin.

(4) Pengamanan Ruang Kantor dan Fasilitasnya

Aturan Kebijakan :

a. Ruangan kerja dan fasilitas di mitratel perlu diberikan pengamanan secara memadai dengan mempertimbangkan pemisahan dari wilayah akses umum.

b. Untuk area kritikal di Mitratel tidak dipasang informasi / petunjuk lokasi yang jelas.

c. Apabila memungkinkan, fasilitas yang digunakan untuk pemrosesan dan penyimpanan informasi sensitif sebaiknya terpisah dengan fasilitas yang digunakan untuk pekerjaan sehari-hari.

d. Dalam mengamankan ruangan tersebut beberapa hal berikut perlu dipertimbangkan :

   1. Perhatian perlu diberikan terhadap aspek kesehatan dan keamanan berdasarkan standar maupun regulasi yang terkait.

   2. Kantor, ruang kerja dan fasilitas Perusahaan perlu didesain sedemikian rupa untuk meminimalisasi akses oleh masyarakat umum.

(5) Perlindungan Terhadap Ancaman Eksternal dan Lingkungan

Aturan Kebijakan :

a. Peralatan pemadam kebakaran yang memadai harus tersedia pada tempat yang sesuai.

b. Khusus ruangan kritikal di Mitratel menggunakan peralatan pemadam kebakaran yang bersifat non-liquid.

c. Perlindungan perlu diberikan kepada area Perusahaan dari Risiko yang muncul dari kebakaran, banjir, gempa bumi, ledakan, huru hara dan bencana lainnya, baik disebabkan oleh alam maupun manusia.

d. Perlindungan tersebut perlu mempertimbangkan kondisi lingkungan sekitar area Perusahaan.

e. Beberapa hal ini perlu dipertimbangkan dalam melaksanaan Proses perlindungan:

   1. Material yang berpotensi menimbulkan bahaya dan mudah terbakar harus di simpan di tempat yang aman dan terpisah dari ruang aktivitas kerja.

   2. Media *Backup* harus disimpan di tempat dengan jarak yang cukup aman dari area Perusahaan untuk menghindari kerusakan apabila terjadi bencana di area Perusahaan.

   3. Memastikan area keamanan khusus memiliki detektor api dan asap serta pipa pembuangan air.

   4. Zat pemadam api dan sistem yang digunakan harus memperhatikan keamanan terhadap peralatan dan petugas pelaksana didalam area TI.

   5. *Data center* dan area yang sensitif yang berisi peralatan komputer yang kritikal dan harus terlindungi oleh deteksi api dan sistem alarm otomatis.

   6. *Data center* harus berada pada lokasi yang lebih tinggi dengan detektor panas,

asap, dan air.

7. Deteksi api dan sistem pemadaman harus diperiksa untuk memastikan bahwa alat tersebut sudah terpasang dengan benar, dan harus diperiksa secara rutin paling sedikit satu kali setiap tahun.
8. Alat pemadam api darurat harus tersedia pada lokasi yang strategis dan mudah untuk dijangkau. Instruksi penggunaannya harus ditampilkan.
9. Dilarang merokok serta membawa makan dan minum dalam area keamanan khusus.

(6) Bekerja di Area Aman

Aturan Kebijakan :

a. Pekerjaan yang dilakukan oleh pihak ketiga di area kritikal di lingkungan Mitratel harus selalu diawasi oleh Karyawan penanggung jawab area tersebut untuk menghindari kegiatan yang tidak diinginkan.
b. Setiap Karyawan dan pihak ketiga dilarang merokok serta membawa makanan dan minuman ke dalam wilayah tertutup.
c. Pihak ketiga yang memasuki wilayah tertutup tidak diperkenankan membawa peralatan visual *recording* (*kamera, handphone berkamera*).
d. Pekerjaan di area keamanan khusus, baik yang dilakukan oleh pihak internal maupun eksternal, memerlukan perlindungan dan panduan khusus untuk mengurangi kemungkinan adanya kecelakaan, insiden atau gangguan dalam bekerja.
e. Pintu masuk dan lokasi penting pada area keamanan khusus harus dilengkapi dengan kamera *closed camera television* (CCTV). Perekam CCTV harus disimpan pada tempat aman, dan hasil rekaman CCTV harus disimpan untuk beberapa waktu tertentu.
f. Area keamanan khusus yang kosong harus selalu terkunci dan secara rutin dilakukan pengecekan.

(7) Area untuk *delivery* dan *loading*

Aturan Kebijakan :

a. Akses di wilayah *loading* area yang dapat memasuki wilayah Mitratel harus diamankan untuk menghindari akses tanpa ijin.
b. Dalam mengamankan area tersebut beberapa hal tersebut perlu dilakukan :
    1. Akses ke area tersebut harus dibatasi untuk Karyawan yang telah terdaftar dan terotorisasi.
    2. *Delivery* dan *loading area* harus ditempatkan dimana Karyawan yang mengakses area tersebut tidak perlu memasuki area terbatas dan tertutup Perusahaan.
    3. Pintu masuk ke *delivery* dan *loading area* harus diamankan.
    4. Barang-barang yang datang dari luar harus didaftarkan dan diperiksa sebelum dipindahkan ke area internal Perusahaan.

Pasal 23
Perangkat

Pengamanan ini diperlukan untuk mencegah kehilangan, kerusakan, pencurian terhadap Aset Informasi atau gangguan terhadap aktivitas.

Pengamanan tersebut diperlukan untuk melindungi peralatan milik Perusahaan dari ancaman fisik dan lingkungan.

(1) Perlindungan dan penempatan peralatan

Aturan Kebijakan :

a. Perangkat pengolahan informasi yang dianggap kritikal perlu ditempatkan secara aman termasuk membatasi sudut pandang untuk mengurangi orang yang tidak berkepentingan yang dapat melihat informasi yang ditampilkan.

b. Peralatan kerja milik Perusahaan harus ditempatkan dan dilindungi untuk mengurangi Risiko ancaman yang berasal dari lingkungan (api, air, debu).

c. Dalam melindungi peralatan kerja milik Perusahaan beberapa hal berikut perlu dipertimbangkan :

1. Penempatan peralatan kerja perlu dilakukan sedemikian rupa untuk mengurangi Risiko adanya akses yang tidak perlu ke area kerja.

2. Fasilitas atau peralatan pengolahan informasi perlu ditempatkan sedemikian rupa sehingga mengurangi pandangan dari orang yang tidak berwenang. Hal ini termasuk membatasi sudut pandang ke peralatan tersebut.

3. Peralatan yang membutuhkan perlindungan khusus dapat diisolasi di lokasi khusus untuk mengurangi jumlah pengamanan yang diperlukan.

4. Kontrol yang memadai harus diterapkan untuk meminimalkan Risiko ancaman gangguan fisik, seperti pencurian, kebakaran, ledakan gangguan dari asap, air, petir, debu, getaran, bahan kimia, gangguan terhadap pasokan listrik, jaringan komunikasi, elektromagnetik dan vandalisasi.

5. Suhu dan kelembaban dalam area keamanan khusus harus dimonitor secara rutin.

6. Perlindungan dari petir perlu diimplementasikan pada bangunan, jalur listrik maupun komunikasi.

(2) Sarana Pendukung

Aturan Kebijakan :

a. Semua sarana pendukung seperti *power supply*, genset, lampu darurat, dan air conditioner harus tersedia untuk mendukung kegiatan operasional Mitratel dan dipelihara serta diperiksa secara berkala untuk memastikan sarana pendukung tersebut dapat berfungsi sebagaimana mestinya.

b. Peralatan pengolahan informasi milik Perusahaan harus dilindungi dari kemungkinan hilangnya pasokan listrik dan gangguan lain yang disebabkan oleh gangguan pada sarana pendukung. Penyediaan penerangan darurat perlu disediakan untuk menjamin penerangan dalam kondisi hilangnya pasokan listrik.

c. Kondisi suplai listrik perlu dipastikan telah sesuai dengan kebutuhan dari peralatan pengolahan informasi.

d. Apabila memungkinkan *emergency power off switches* dapat digunakan untuk mematikan dengan segera peralatan pengolahan informasi seandainya terjadi kondisi darurat.

e. Ketersediaan bahan bakar pada generator listrik harus dipastikan untuk mencukupi kebutuhan pada saat diperlukan.

f. Bila memungkinkan penggunaan beberapa sumber pasokan listrik dapat diimplementasikan terutama untuk peralatan pengolahan informasi yang sangat sensitif untuk mengurangi kegagalan operasi pada peralatan pengolahan informasi apabila pasokan listrik yang ada putus (*single point of failure*).

g. Sumber Daya Listrik di-*backup* oleh *uninterrupted power supply* ("UPS") dan generator, dengan Prosedur yang meliputi hal-hal berikut:

   1. *Generator* harus terpasang untuk mendukung penyediaan listrik *data center.*
   2. Sumber Daya Listrik harus didukung oleh *UPS* atau batere cadangan, dan harus mampu untuk mendukung kapasitas untuk periode sekurang-kurangnya 15 (lima belas) menit pada saat terjadi pemadaman listrik.
   3. Ruang *generator* dan UPS harus aman dan terkunci. Kunci harus disimpan dan hanya dapat diberikan kepada petugas yang ditunjuk.
   4. Ruang *generator* dan UPS harus mempunyai ventilasi yang memadai dan dilengkapi dengan sistem deteksi dan perlindungan api.

h. *Generator* dan UPS harus dipelihara dan dijaga ketersediaannya secara periodik, minimal satu bulan sekali, dan dilakukan pengetesan minimal tiga bulan sekali.

i. Pasokan air untuk peralatan AC dan pemadam kebakaran perlu dipastikan ketersediaanya. Terkait dengan Proses pemadam kebakaran, sistem peringatan (*alarm*) juga harus diperiksa secara rutin

j. Penyediaan jalur telekomunikasi ganda dari sisi *routing,* penyedia jaringan atau teknologi jaringan perlu dipertimbangkan untuk mengurangi Risiko kegagalan komunikasi apabila salah satu jalur telekomunikasi yang ada terputus (*single point of failure*).

(3) Pengamanan pengkabelan

Aturan Kebijakan :

a. Kabel listrik dan jaringan komunikasi harus terlindungi dan tidak diletakkan di area publik sehingga tidak mengalami kerusakan akibat ketidaksengajaan oleh Karyawan maupun gigitan binatang pengerat.

b. Penandaan kabel digunakan di ruang server jaringan untuk mempermudah penanganan apabila terjadi masalah dan menghindari kesalahan dan didokumentasikan dengan baik.

c. Pengamanan pengkabelan perlu mempertimbangkan beberapa hal berikut:

1. Kabel listrik dan telekomunikasi yang digunakan untuk fasilitas pemrosesan informasi harus dipasang secara aman sedemikian rupa sehingga dapat terlindung dengan baik.
2. Kabel komunikasi harus terlindungi dari kemungkinan kerusakan maupun intersepsi seperti dengan tidak diletakkan di area publik.
3. Kabel listrik harus terpasang secara terpisah dengan kabel komunikasi.
4. Untuk sistem kritikal atau sensitif perlindungan tambahan sebagai berikut dapat dilakukan :
   (a) Penggunaan pelindung kabel (*armoured conduit*) dan kotak atau ruangan terkunci untuk melindungi kabel terutama pada titik terminasi atau pemeriksaan.
   (b) Penggunaan *routing* maupun media transmisi alternatif
   (c) Penggunaan kabel *fiber optic.*
   (d) Penggunaan pelindung elektromagnetik
   (e) Pemeriksaan teknis secara fisik untuk memastikan tidak ada peralatan yang seharusnya tidak terhubung ke sistem komunikasi.
   (f) Pengendalian akses ke ruangan kabel dan *patch panel.*

(4) Pemeliharaan peralatan

Aturan Kebijakan :

a. Peralatan sistem informasi seperti perangkat keras dan jaringan komunikasi, serta sarana pendukung harus dipelihara untuk menjamin ketersediaan dan integritas dari peralatan tersebut secara terus menerus.
b. Dalam melakukan pemeliharaan peralatan dalam sistem informasi Perusahaan, beberapa hal berikut perlu dipertimbangkan:
   1. Melakukan pemeliharaan peralatan secara rutin sesuai spesifikasi dan rekomendasi vendor.
   2. Aktivitas pemeliharaan hanya boleh dilakukan oleh Karyawan yang memiliki kompetensi dan mendapat izin dari pihak yang pengelola perangkat.
   3. Setiap indikasi kerusakan, kerusakan yang terjadi serta perbaikan yang bersifat korektif dan preventif harus didokumentasikan dengan baik.
   4. Setiap pemeliharaan perlu mempertimbangkan informasi yang terdapat didalam dalam peralatan tersebut.

(5) Pemindahan Peralatan Milik Mitratel

Aturan Kebijakan :

a. Peralatan, informasi, maupun perangkat lunak milik Mitratel atau milik pihak ekternal yang diserahkan pengelolaannya kepada Mitratel tidak boleh di bawa keluar wilayah Mitratel tanpa adanya ijin dari Pejabat dari Unit terkait yang mengelola fungsi Perangkat, informasi maupun perangkat lunak di Mitratel.

b. Dalam memastikan Proses kendali keamanan beberapa hal berikut perlu dipertimbangkan:

1. Aset hanya dapat dibawa keluar area Perusahaan oleh pihak yang diberikan otorisasi resmi.
2. Aset yang dibawa keluar harus didokumentasikan dengan baik.
3. Apabila diperlukan, pemeriksaan dapat dilakukan terhadap personel yang keluar dari area Perusahaan.

(6) Pengamanan peralatan diluar wilayah Mitratel

Aturan Kebijakan :

a. Penggunaan peralatan pengolahan informasi di luar wilayah Mitratel mempertimbangkan kebutuhan penggunaan aset tersebut.

b. Aset TI yang bersifat portabel seperti notebook yang dibawa ke luar area kantor tidak boleh ditinggalkan di area publik tanpa pengamanan yang memadai dengan kabel pengunci (*cable lock*) serta *password*.

c. Pengamanan harus dilakukan pada semua terletak diluar area Perusahaan (*off premises*). Pengamanan ini perlu mempertimbangkan Risiko yang muncul dari penggunaan peralatan dan pekerjaan diluar area Perusahaan.

d. Penggunaan peralatan pengolahan informasi diluar area Perusahaan harus mendapatkan ijin dari pihak pengelola/pemilik peralatan.

e. Dalam menerapkan pengamanan, hal-hal berikut perlu dipertimbangkan :

1. Informasi dan peralatan pengolahan informasi tidak boleh ditinggal di area umum tanpa pengawasan.
2. Instruksi dari vendor pembuat peralatan pengolahan informasi mengenai penggunaan peralatan tersebut harus dipatuhi.
3. Pengendalian keamanan bagi peralatan yang digunakan untuk bekerja dari rumah perlu melalui Proses penilaian Risiko untuk menentukan metode kendali keamanan yang tepat.
4. Penggunaan jasa asuransi untuk melindungi perusahaan dari kerugian yang mungkin muncul dari penggunaan peralatan diluar area perusahaan.

(7) Pemusnahan atau Penggunaan Kembali Peralatan Secara Aman

Aturan Kebijakan :

a. Seluruh Aset TI yang akan dimusnahkan atau digunakan kembali harus diperiksa dan dipastikan bahwa tidak ada lagi data sensitif yang tersimpan dalam perangkat sehingga tidak dimungkinkan lagi untuk mengambil informasi yang sebelumnya terkandung di perangkat tersebut.

b. Peralatan pengolahan informasi yang tidak akan dipergunakan lagi dan di dalamnya terdapat informasi sensitif harus dimusnahkan secara fisik, dihapus secara permanen sehingga tidak dimungkinkan lagi untuk mengambil informasi yang sebelumnya terkandung dalam peralatan tersebut.

c. Peralatan pengolahan informasi yang akan diperbaiki atau digunakan kembali perlu dipastikan bahwa tidak ada informasi sensitif yang masih terkandung sebelum peralatan tersebut diperbaiki atau digunakan kembali.

(8) Perlindungan untuk perangkat yang tidak dalam pengawasannya

Aturan Kebijakan :

a. Pengguna harus memastikan aset yang sedang tidak digunakan telah terlindungi dengan baik dengan menghentikan (*terminate*) *session* aktif terhadap sistem setelah selesai digunakan.

b. Sedapat mungkin melakukan *log-off* pada komputer atau server setelah *session* selesai digunakan.

c. Mengamankan komputer atau terminal yang digunakan dengan menggunakan *password.*

(9) *Clear desk* dan *clear screen*

Aturan Kebijakan :

a. Seluruh Karyawan Mitratel harus menerapkan *clear desk* dan *clear screen* terkait dengan Keamanan Informasi yang rahasia atau sensitif.

b. Semua informasi sensitif yang berbentuk *hardcopy* atau yang tersimpan dalam media penyimpanan dalam lemari yang terkunci.

c. Komputer atau terminal harus di *log-off* / *screen saver lock* apabila sedang tidak digunakan atau diawasi.

d. Memindahkan dengan segera dokumen yang mengandung informasi sensitif dari mesin *printer* maupun *foto copy.*

e. Pengamanan pada tempat pengiriman dan penerimaan surat dan mesin *faximile* yang tidak diawasi.

Pasal 24
Saling Ketergantungan Vertikal dan Horizontal

Proses ini berkaitan dengan hubungan rumit antara komponen yang telah diidentifikasi sebagai penting antara, serta dan di dalam organisasi – pada dasarnya, antar serta intra organisasi. Infrastruktur Informasi Vital Tidak dapat dilihat secara terpisah dan semua ketergantungan vertikal dan horizontal dengan atau sumber daya lain harus dipertimbangkan.

Aturan Kebijakan :

(1) Saling ketergantungan vertikal mengacu pada hubungan simbiosis antara lapisan organisasi (yaitu saling ketergantungan Unit Kerja) dalam suatu organisasi dan antara organisasi dan anak Perusahaan, jika ada.

(2) Identifikasi dan pemahaman tentang keterkaitan merupakan kebutuhan mutlak untuk membangun lingkungan yang aman dalam Infrastruktur Informasi Vital.

(3) Interdependensi horizontal, didasarkan pada Interdependensi masuk dan keluar. *In-bound* interdependensi mencakup peran dan Layanan yang diharapkan dari suatu Unit kerja oleh Unit Kerjan lain.

(4) Ketergantungan *out-bound* mencakup harapan Layanan oleh satu Unit Kerja tertentu dari yang lain. Atas dasar dependensi masuk dan keluar, Infrastruktur Informasi Vital secara keseluruhan harus ditetapkan dan pendekatan holistik akan diadopsi untuk keamanan.

Pasal 25
Sertifikasi Keamanan

Sertifikasi keamanan berkaitan dengan validasi langkah-langkah keamanan atau Kontrol yang diambil oleh Infrastruktur Informasi Vital untuk melindungi Aset Informasi agar operasi lancar dan bebas kesalahan. Validasi ini dilakukan oleh instansi pihak ketiga yang dapat berupa instansi pemerintah maupun swasta. Sertifikasi juga harus berurusan dengan penegakan atau penerapan standar keamanan internasional yang tersedia secara global untuk perlindungan Aset Informasi penting yang bekerja pada masing-masing Unit.

Aturan Kebijakan :

(1) Setiap Infrastruktur Informasi Vital perlu menyusun strategi untuk membuat daftar sertifikasi yang perlu diterapkan untuk melindungi Aset Informasi.

(2) Serupa dengan sertifikasi fasilitas Infrastruktur Informasi Vital, ada persyaratan untuk memastikan bahwa Karyawan memiliki sertifikasi yang relevan dengan tanggung jawab.

(3) Persyaratan sertifikasi keamanan dari Karyawan yang terlibat dalam pekerjaan perlindungan di berbagai tingkat dan bidang harus ditulis dengan jelas.

(4) Program peningkatan pengetahuan bagi Karyawan melalui sertifikasi baru, pelatihan, seminar, lokakarya juga harus direncanakan sesuai kebutuhan masing-masing Infrastruktur Informasi Vital.

(5) Proses peninjauan dan umpan balik mengenai induksi atau penghapusan sertifikasi keamanan untuk Aset Informasi dan Karyawan harus dilakukan secara berkala.

(6) Proses implementasi sertifikasi keamanan harus dipantau dengan baik oleh manajemen sehingga Prosedur tersebut tidak mempengaruhi fungsi normal Infrastruktur Informasi Vital.

Pasal 26
Penerapan Arsitektur yang Aman dan Handal

Penerapan arsitektur yang aman mengacu pada pembentukan dan pelaksanaan arsitektur Informasi dan jaringan yang aman dan terjamin dalam organisasi atau Infrastruktur Informasi Vital sesuai dengan kebijakan Keamanan Informasi dari Infrastruktur Informasi Vital terkait, dengan tetap memperhatikan keseimbangan antara Bisnis/Layanan, Informasi, Teknologi dan arsitektur keamanan.

(1) Pembentukan Arsitektur

Aturan Kebijakan :

a. Arsitektur yang aman sebelum finalisasi harus menyediakan taksonomi dan ontologi yang ketat dalam mengidentifikasi secara jelas mengenai peran, tanggung jawab, proses, dan jaringan yang akan diimplementasikan yang paling sesuai dengan persyaratan Keamanan Informasi bersama dengan kebutuhan fungsional Infrastruktur Informasi Vital dengan tetap memperhatikan Informasi, keamanan, Layanan/Bisnis

dan arsitektur teknologi.

b. Dalam penerapan arsitektur aman, komponen TI seperti aliran proses, pengaturan waktu organisasi, aplikasi dan inventaris perangkat lunak, peristiwa, pesan, aliran data, intranet, extranet, internet, *e-Commerce*, klasifikasi data, database, server, komponen jaringan, perangkat keamanan, *local area network* (LAN), *wide area network* (WAN), secara eksplisit terkait dengan strategi, tujuan, dan operasi organisasi.

c. Tidak diterapkannya Kontrol ini dapat memiliki implikasi besar dalam kesuksesan implementasi kebijakan Keamanan Informasi yang merupakan bagian dari Infrastruktur Informasi Vital.

(2) Pelakasanaan Arsitektur

Aturan Kebijakan :

a. Harus ada rencana penyebaran arsitektur yang aman dan tangguh dalam kebijakan Informasi yang spesifik untuk kebutuhan dan fungsi Infrastruktur Informasi Vital.

b. Arsitektur jaringan harus memasukkan keamanan sebagai elemen desain utama.

c. Arsitektur keseluruhan yang terdiri dari sistem TI, produk beserta pemilihannya dan kondisi penerapannya harus dianalisis dan diperiksa sepenuhnya dengan tetap memperhatikan keamanan Informasi Infrastruktur Informasi Vital.

d. Pemilihan arsitektur harus mencapai keseimbangan antara keamanan dan persyaratan bisnis.

e. Peningkatan otomatis dan pemantauan log juga harus menjadi bagian dari penyebaran arsitektur yang aman.

f. Pengujian dan evaluasi Kontrol industri, dan produk otomasi harus dilakukan sebelum diterapkan dalam arsitektur Infrastruktur Informasi Vital, dengan mempertimbangkan Keamanan Informasi.

g. Pengerasan semua sistem dan produk TI juga harus tercakup dalam penerapan arsitektur yang aman.

h. Arsitektur harus mudah beradaptasi dan dapat ditingkatkan sejalan dengan perubahan cepat dalam teknologi dan tren Keamanan Informasi.

i. Arsitektur harus dirancang, dengan mempertimbangkan keamanan sistem informasi yang digunakan melalui pemantauan dan analisis, audit reguler dan pentest yang akan membantu sistem untuk tahan terhadap serangan *Cyber*.

j. Sistem komunikasi kritis dan saluran komunikasinya harus dilindungi untuk menghindari penyadapan yang dapat dilakukan dengan menggunakan *Secure Socket Layer* (SSL) atau https di *Uniform Resource Locators* (URL).

BAB VIII
Keamanan Operasional

Pasal 27
Tanggung Jawab dan Prosedur Operasional

Kendali sistem keamanan ini berfungsi untuk memastikan bahwa Proses operasional fasilitas pengolahan informasi berjalan dengan benar dan aman.

Hal ini dapat diimplementasikan dengan pengalokasian tanggung jawab, pembuatan Prosedur pengelolaan dan operasional fasilitas pengolahan informasi dan memastikan bahwa pemisahan tugas (*segregation of duties*) telah dilakukan.

(1) Prosedur Operasional Yang Terdokumentasi

Aturan Kebijakan :

a. Setiap sistem yang dioperasikan di Mitratel harus dilengkapi dengan Prosedur dan petunjuk pengoperasian (sebagai contoh *run book* dan petunjuk teknis) dan dipelihara untuk menjaga ketersediaan bagi seluruh Pengguna sistem informasi yang membutuhkannya.

b. Prosedur operasional perlu secara spesifik memberikan detail mengenai pelaksanaan kegiatan yang mencakup :

   1. Pengelolaan dan pengolahan sistem informasi
   2. *Backup*
   3. Penjadwalan aktivitas kerja, hal ini perlu mempertimbangkan ketergantungan antar sistem.
   4. Prosedur penanganan kesalahan / gangguan selama aktivitas pekerjaan berlangsung.
   5. Pihak yang harus dihubungi untuk mendapatkan dukungan (*support*) apabila terjadi masalah atau kesulitan.
   6. Prosedur *restart* dan *recovery* sistem.
   7. Pengelolaan *audit trail* dan *log* sistem.

c. Seluruh dokumentasi dari Prosedur operasional harus ditangani sesuai klasifikasinya dan sesuai dengan Proses pengelolaan dokumentasi Perusahaan.

(2) Manajemen Perubahan

Aturan Kebijakan :

a. Seluruh perubahan dalam infrastruktur TI dan sistem aplikasi harus dikelola dan dikendalikan untuk menghindari terjadinya kegagalan dalam sistem informasi.

b. Pengendalian perubahan diterapkan pada infrastruktur dan Sistem harus mengacu pada Prosedur yang mempertimbangkan antara lain:

   1. Aspek Risiko yang muncul terhadap kebutuhan bisnis.
   2. Dokumentasi atas log perubahan sesuai urutan waktu perubahan.

3. Perencanaan dan pengujian perubahan.
4. Tersedianya persetujuan formal untuk usulan perubahan
5. Review dan pemantauan terhadap pelaksanaan perubahan.

c. Seluruh sistem operasional dan aplikasi perangkat lunak harus dikelola dan dikendalikan melalui Manajemen perubahan yang formal.

d. Berdasarkan tingkat kepentingannya, perubahan digolongkan menjadi :

1. Perubahan terencana, adalah perubahan yang telah direncanakan terlebih dahulu.
2. Perubahan darurat, dibutuhkan untuk memperbaiki permasalahan pada sistem TI untuk mengembalikan Proses operasional dengan cepat dan harus mendapatkan persetujuan dari pengelola sistem TI yang berwenang.

e. Manajemen perubahan perlu mencakup namun tidak terbatas pada :

1. *Assesment* dari potensi dampak, termasuk dampak dari sisi keamanan yang mungkin muncul dari perubahan.
2. Prosedur persetujuan secara formal untuk setiap perubahan.
3. Komunikasi seluruh detail dari perubahan kepada Karyawan yang relevan
4. Prosedur *fall back*, hal ini mencakup tanggung jawab dan Prosedur untuk membatalkan dan pemulihan dari perubahan yang gagal dan kejadian yang tidak terduga sebelumnya.

f. Setiap perubahan yang dilakukan perlu disetujui dan didokumentasikan.

(3) Manajemen Kapasitas

Aturan Kebijakan :

a. Setiap penanggung jawab sistem di Unit Kerja yang mengelola fungsi TI harus melakukan manajemen kapasitas untuk setiap pengembangan infrastruktur dan sistem aplikasi baru maupun yang sedang berjalan dengan mempertimbangkan proyeksi terhadap kebutuhan operasional, dan infrastruktur berdasarkan kebutuhan bisnis yang akan datang dan sistem informasi Perusahaan. Selain itu proyeksi tersebut perlu juga mempertimbangkan kondisi sistem informasi Perusahaan saat ini dan tren proyeksi perkembangan sistem selama ini.

b. Pengukuran kapasitas terhadap aplikasi dan infrastruktur dilakukan secara periodik.

c. Penggunaan seluruh sumber daya pengolahan informasi dalam sistem informasi Perusahaan harus dipantau, dilakukan Proses *tuning* untuk menjamin kinerja sistem yang diharapkan dapat selalu tersedia dan tidak terjadinya kegagalan sistem karena kapasitas yang tidak mencukupi.

d. Semua aktivitas atau Proses dalam sistem informasi baik yang sedang berjalan maupun yang akan dijalankan harus mengidentifikasi *item* kebutuhan kapasitas sistem, sebagai contoh adalah kapasitas memori atau *storage* dalam *server,* utilisasi CPU *server* atau utilisasi *backbone jaringan Wide Area Network* (WAN) .

e. Dalam Proses Manajemen kapasitas perhatian lebih perlu diberikan untuk sistem atau perangkat pengolahan informasi yang memiliki biaya tinggi secara finansial, waktu maupun penggunaan sumber daya manusia. Untuk sistem dengan biaya tinggi tersebut Unit Kerja yang mengelola fungsi TI sebagai pemilik sistem perlu memantau secara seksama penggunaan dan utilisasi sistem.

f. Proses Manajemen kapasitas juga perlu mempertimbangkan adanya ketergantungan atau *bottleneck* terkait sumber daya manusia yang dapat menimbulkan ancaman terhadap aspek kerahasiaan, integritas maupun ketersediaan informasi dan sistem informasi Perusahaan.

(4) Pemisahan Lingkungan Pengembangan, Pengujian, dan Operasional

a. Fasilitas sistem pengembangan, pengujian dan operasional harus dipisahkan untuk mengurangi Risiko akses atau perubahan tanpa ijin / tidak disengaja pada sistem operasional.

b. Tingkat pemisahan antara lingkungan pengembangan, pengujian dan operasional harus diidentifikasi dan pengendalian untuk menjamin terjaganya pemisahan tersebut harus diterapkan.

c. Hal-hal berikut perlu dipertimbangkan dalam Proses pemisahan tersebut :

1. Prosedur untuk memindahkan perangkat lunak dari lingkungan pengembangan (*development*) ke lingkungan operasional (*production*) harus ditetapkan dan didokumentasikan dengan jelas.

2. Perangkat lunak atau aplikasi yang digunakan untuk lingkungan pengembangan dan operasional harus dijalankan pada sistem atau perangkat keras yang terpisah. Pemisahan tersebut dapat dilakukan secara fisik maupun secara *logical.*

3. *Compiler*, *editor*, dan *tools* pengembangan lain tidak diperbolehkan untuk diakses dari sistem operasional kecuali sangat dibutuhkan.

4. Apabila memungkinkan lingkungan pengujian harus memiliki kesamaan, baik dari sisi konfigurasi maupun spesifikasi, dengan lingkungan operasional.

5. Pengguna harus menggunakan profil Pengguna yang berbeda ketika menjalankan sistem pada lingkungan operasional dan pengujian.

6. Menu-menu dalam aplikasi harus menampilkan keterangan yang jelas untuk meminimalkan kesalahan Pengguna dalam membedakan lingkungan sistem yang ada.

7. Data-data yang bersifat sensitif tidak diperbolehkan disalin (*copy*) ke lingkungan pengujian tanpa pengamanan yang memadai.

Pasal 28
Ulasan Berkala

(1) Bahwa untuk memastikan kepatuhan Karyawan atau pihak ketiga/pihak terkait lainnya dengan Peraturan ini, akan dilakukan evaluasi atau tinjauan secara berkala setiap 1 (satu) tahun oleh Unit Yang Mengelola Fungsi TI. Tinjauan ini akan mencakup pengujian terhadap tingkat kepatuhan terhadap Peraturan ini.

(2) Bahwa evaluasi atau tinjauan berkala sebagaimana ayat (1) Pasal ini, untuk memastikan kesesuaian dan efektivitas Peraturan ini. Tinjauan ini dapat mengakibatkan modifikasi, penambahan, penyesuaian kembali terkait dengan kebijakan keamanan data sehingga lebih sesuai dengan kebutuhan Perusahaan.

Pasal 29
Penutup

(1) Bahwa Peraturan ini sekaligus mengesahkan tata kebijakan keamanan Informasi Perusahaan baik lingkup internal dan/atau lingkup eksternal.

(2) Bahwa apabila terdapat hal-hal yang belum atau belum cukup diatur dalam Peraturan ini, maka akan ditetapkan dan diatur lebih lanjut baik melalui perubahan atau penambahan dalam bentuk amandemen ataupun addendum terhadap Peraturan ini.

(3) Bahwa Peraturan ini mulai berlaku sejak tanggal ditetapkan.

Ditetapkan di : Jakarta

Pada Tanggal : 31 Januari 2022

a.n. Direksi PT Dayamitra Telekomunikasi Tbk
PT DAYAMITRA TELEKOMUNIKASI Tbk

THEODORUS ARDI HARTOKO
DIREKTUR UTAMA