



STANDAR PROSEDUR OPERASIONAL PENGELOLAAN TEKNOLOGI INFORMASI

NOMOR REGISTRASI: 001/2023/SPO/RSC

RISK, SYSTEM & COMPLIANCE

2022

Standar Pedoman Operasional ini dimaksudkan untuk digunakan oleh PT UG Mandiri.

Dilarang memperbanyak baik sebagian maupun seluruhnya dalam bentuk dan cara apapun (cetakan, copy elektronik dsb), disimpan dalam media apapun tanpa persetujuan tertulis dari PT UG Mandiri atau karena perintah Undang-Undang

**Standar Prosedur Operasional
Pengelolaan Teknologi Informasi**

Lembar Persetujuan



Disusun oleh:

Nama	Jabatan	Unit Kerja	Tanda Tangan	Tanggal
Rahmat Setiawan	Manager System & Procedure	Risk System & Compliance (RSC)		9/01/2023

Dikaji oleh:

Nama	Jabatan	Unit Kerja	Tanda Tangan	Tanggal
Reko Afiantoro	Manager IT Support	Risk, System & Compliance (RSC)		13/01/2023
Endang Pariyanto	Manager Risk Management & Compliance			18/01/2023
Eko Ervan	General Manager RSC			19/01/2023
Haris Triyadi	Executive General Manager Finance & Support			20/01/2023

Disetujui oleh:

Nama	Jabatan	Tanda Tangan	Tanggal
Hargo Hadi	Direktur Building, Construction & Support Management		27/01/2023
Sugeng Hariadi	Direktur Utama		27/01/2023

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :
Tgl Berlaku :		Revisi :	

**Standar Prosedur Operasional
Pengelolaan Teknologi Informasi (TI)**

Kata Pengantar



Standar Prosedur Operasional (SPO) Pengelolaan Teknologi Informasi (TI) Pegawai disusun sebagai pedoman dalam melaksanakan Pengelolaan Teknologi Informasi di lingkungan PT Usaha Gedung Mandiri (PT UG Mandiri).

Setiap Pegawai PT UG Mandiri harus memahami, melaksanakan serta mematuhi isi SPO, sehingga diperoleh pemahaman tentang ketentuan dan pelaksanaan Pengelolaan Teknologi Informasi (IT Support).

SPO No.001/2023/SPO/RSC tanggal 27 Januari 2023 ini adalah merupakan penyempurnaan dari versi sebelumnya dengan No.004/2022/SPO/RSC tanggal 24 November 2022 sesuai yang disyaratkan dan standarisasi ISO 27001 : 2013 perihal Standar Sistem Manajemen Keamanan Informasi. Penyempurnaan yang dilakukan didasarkan adanya pengembangan proses dan masukan berbagai pihak sehingga SPO ini mudah dipahami dan diaplikasikan dalam pekerjaan sehari-hari.

SPO ini hanya boleh digunakan dalam lingkungan kantor PT UG Mandiri. Tidak diperkenankan untuk dicetak ulang, difotocopy, diperbanyak atau dimiliki oleh pihak-pihak yang tidak berhubungan dengan PT UG Mandiri tanpa persetujuan tertulis dari Direksi. Setiap unit kerja atau pegawai yang menggunakan SPO Pengelolaan Teknologi Informasi harus bertanggungjawab atas pemeliharaan maupun penyimpanannya dengan tertib.

Demikian, agar SPO ini menjadi standar pedoman dalam Pelaksanaan Pengelolaan Teknologi Informasi (IT Support) serta acuan dalam melaksanakan pengelolaan Teknologi Informasi di PT UG Mandiri.

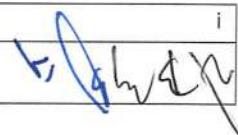
Diterbitkan di Jakarta, 27 Januari 2023

✓ PT Usaha Gedung Mandiri



Sugeng Hariadi
Direktur Utama

Hargo Hadi
Direktur

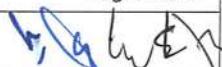


KATA PENGANTAR

Halaman
i
1

DAFTAR ISI

	Halaman
Bab I. PENDAHULUAN	
A. Latar Belakang	3
B. Maksud dan Tujuan	3
C. Dasar Penyusunan	3
D. Ruang Lingkup	4
E. Daftar Istilah	4
Bab II. ORGANISASI IT SUPPORT	
A. Organisasi Satuan Kerja IT Support	6
B. Struktur Organisasi	6
1. Satuan Kerja yang menangani Pengembangan Aplikasi IT	7
2. Satuan Kerja yang menangani Operasional dan Infrastruktur TI	7
3. Satuan Kerja yang menangani Keamanan Sistem Informasi TI	8
4. Satuan Kerja yang menangani Media Sosial	8
C. Evaluasi Organisasi IT Support	8
Bab III. TATA KELOLA TEKNOLOGI INFORMASI	
A. Penyelenggaraan dan Pengelolaan Teknologi Informasi	10
B. Wewenang	10
C. Tanggung Jawab	11
D. Pegawai/ User	11
E. Komputer dan Hak Akses	11
F. Aset Perusahaan	12
G. Keamanan Server	12
H. Keamanan Hardware	12
I. Keamanan Cloud Storage	12
J. Keamanan Jaringan Komunikasi Komputer dan Aplikasi Terapan	13
K. Ketentuan Aplikasi Terapan Perusahaan	13
L. Larangan	13
M. Sanksi	13
Bab IV. KETAHANAN SIBER	
A. Jenis Ancaman Siber	14
B. Bentuk Ancaman Siber	14
C. Penanggulangan Serangan Siber	16
D. Pengelolaan Ancaman	16
Bab V. FUNGSI TEKNOLOGI INFORMASI	
A. Ketentuan IT <i>Security Policy</i>	18
B. Ketentuan Pengembangan Sistem	20
C. Ketentuan <i>log</i> dan Pemantauan	21
D. Ketentuan Insiden Keamanan Informasi	23
E. Ketentuan Kontrol Akses	25
F. Ketentuan IT Continuity	27

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 1 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

Standar Prosedur Operasional Pengelolaan Teknologi Informasi (TI) Daftar Isi	 <i>serve you better</i>
---	--

G.	Ketentuan Operasional Teknologi Informasi	28
H.	Ketentuan Wi-Fi	31
I.	Ketentuan Insiden Keamanan Informasi	33
Bab VI.	KEAMANAN FISIK	
A.	Risiko Keamanan Fisik	35
B.	Kontrol Keamanan Fisik	35
Bab VII.	MANAJEMEN PERUBAHAN TI	
A.	Proses Manajemen Perubahan	38
B.	Implementasi Teknologi	38
C.	Peran Teknologi Informasi	39
Bab VIII.	MULTI FACTOR AUTHENTICATION (MFA)	
A.	Metode Autentifikasi	40
B.	Metode Verifikasi yang tersedia	40
C.	Manfaat Multi Factor Authentication	41
Bab IX.	HARDENING SYSTEM	
A.	Pengertian Host Hardening	42
B.	Macam-macam & Implementasi Hardening System	42
C.	Security Hardening	44
D.	System Configuration Hardening	46
Bab X.	KEAMANAN DATA	
A.	Ketentuan Antivirus	50
B.	Ketentuan Removable Media	51
C.	Ketentuan Backup Data	51
D.	Ketentuan Keamanan Penyalinan Data	53
E.	Ketentuan Komputer Seluler	53
Bab XI.	KEY ENCRYPTION	
A.	Manfaat Enkripsi	55
B.	Key Encryption	55
C.	Tipe Enkripsi	56
D.	Penerapan Enkripsi	57
Bab XII.	KONTROL AKSES	
A.	Strategi Kontrol Akses	58
B.	Model Akses Perusahaan	59
Bab XIII.	ANALISA MANAJEMEN RISIKO	
A.	Risiko dan Mitigasi	60
B.	Penutup	61

A. Latar Belakang

Diperlukan ketentuan Pengelolaan Teknologi Informasi sesuai kondisi lingkungan eksternal dan internal perusahaan dengan pertimbangan efisiensi biaya operasional perusahaan.

B. Maksud dan Tujuan

1. Memberikan dukungan agar pemanfaatan teknologi informasi secara optimal atas kegiatan teknologi informasi perusahaan antara lain:
 - a. Terselenggaranya proses *database* perusahaan tersedia secara cepat, tepat dan akurat serta tersentralisasi dan terintegrasi.
 - b. Meningkatkan kemampuan sebagai perencana dan pengendali jalannya operasional perusahaan berbasis IT yang dilaksanakan di unit kerja.
2. Memfasilitasi kemajuan teknologi informasi baik *hardware* maupun *software* yang digunakan perusahaan.
3. Sebagai pedoman bagi pemeliharaan jaringan komputer perusahaan yang efektif, efisien, dan sesuai dengan aturan yang berlaku.
4. Sebagai pedoman perlindungan Aset perusahaan bidang teknologi informasi, data dan informasi, perangkat lunak, perangkat keras, pengguna, dan prosedur-prosedur yang berkaitan.

C. Dasar Penyusunan

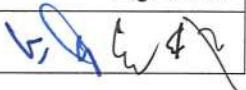
1. *Good Corporate Governance* - PT Usaha Gedung Mandiri No.1048/DIR/XII/2017 tgl. 29 Desember 2017.
2. *Code of Conduct* – PT Usaha Gedung Mandiri No.1049/DIR/XII/2017 tgl. 29 Desember 2017.
3. ISO 27001 : 2013 perihal Standar Sistem Manajemen Keamanan Informasi.
4. SPO No.004/2022/SPO/RSC perihal Pengelolaan Teknologi Informasi

D. Ruang Lingkup

Pengelolaan *hardware* , *software*, jaringan/ *network*, ketahanan siber, *database*, *server*, media sosial di perusahaan.

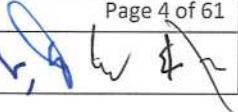
E. Daftar Istilah

1. Administrator : Pegawai/ petugas yang ditunjuk dan diberi wewenang oleh perusahaan untuk mengelola *server*, *hub broadband satelite* dan hak akses *user*.
2. Divisi : Organ perusahaan yang terdiri dari seluruh Divisi yang ditentukan berdasarkan Surat Keputusan Direksi (SKD) antara lain adalah Sekretaris Perusahaan, Satuan Pengawasan Intern, Hukum, Pemasaran, Pengembangan, Umum dan Pengadaan, Keuangan dan Akuntansi, Sumber Daya Manusia,, Jasa Penunjang dan *log*

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 3 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

istik.

3. *Hardware* : Perangkat keras teknologi informasi antara lain *radio/wireless link, modem, server, router, komputer, printer, scanner, switch hub*, kabel LAN, stabilisator dan UPS yang dipergunakan untuk mendukung kelancaran operasional teknologi informasi.
4. *Intranet* : Jaringan komputer yang menghubungkan antar komputer/*server* dalam satu jaringan komputer di satu tempat tertentu dengan komputer/*server* dalam satu jaringan komputer di tempat lain.
5. *Internet* : Jaringan komputer menghubungkan antar komputer/*server* dalam satu jaringan komputer perusahaan dengan komputer/*server* pada jaringan komputer di luar perusahaan.
6. *Jaringan* : Sebuah sistem yang terdiri atas *Local Area Network (LAN)*, intranet, dan internet serta perangkat lain yang bekerja bersama-sama, untuk mengkoneksikan antar komputer dengan *server* pada satu tempat atau di lain tempat tertentu.
7. *Local Area Network (LAN)* : Jaringan komputer yang menghubungkan antar komputer/*server* melalui kabel atau *radio/wireless* dalam satu lokasi tertentu.
8. *Programmer* : Pegawai yang ditunjuk dan diberi wewenang oleh perusahaan untuk merencanakan, membangun, mengembangkan, memelihara program aplikasi komputer.
9. *Software* : Perangkat lunak teknologi informasi berupa sistem operasi komputer (*operating System*), aplikasi umum, aplikasi *tools*, aplikasi multimedia, internet dan aplikasi internal yang digunakan untuk mendukung operasional *hardware* dan jaringan teknologi informasi.
10. *Software Sistem Operasi* : Perangkat lunak yang digunakan untuk mengatur sumber daya *hardware* dan *software* aplikasi agar dapat beroperasi sebagaimana mestinya, misalnya *Windows*, dll.
11. *Software Aplikasi Umum* : Perangkat lunak yang digunakan pada komputer/*server* atau perangkat keras lainnya untuk keperluan pengolahan kata, *table, database, presentasi* misalnya MS Office, dll.
12. *Software Tools* : Perangkat lunak fungsi tertentu yang digunakan untuk melakukan pemeriksaan perangkat keras, memeriksa kerusakan *hard disk*/media penyimpanan data dan pembangunan aplikasi internal serta *database*, misalnya Norton Utility, Ccleaner dll.
13. *Software Aplikasi Multimedia* : Perangkat lunak yang digunakan untuk menjalankan *file / data* yang berjenis multimedia misalnya Winamp, *Media player*,

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 4 of 61
No Reg :	001/2023/SPO/RSC	Edisi :02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

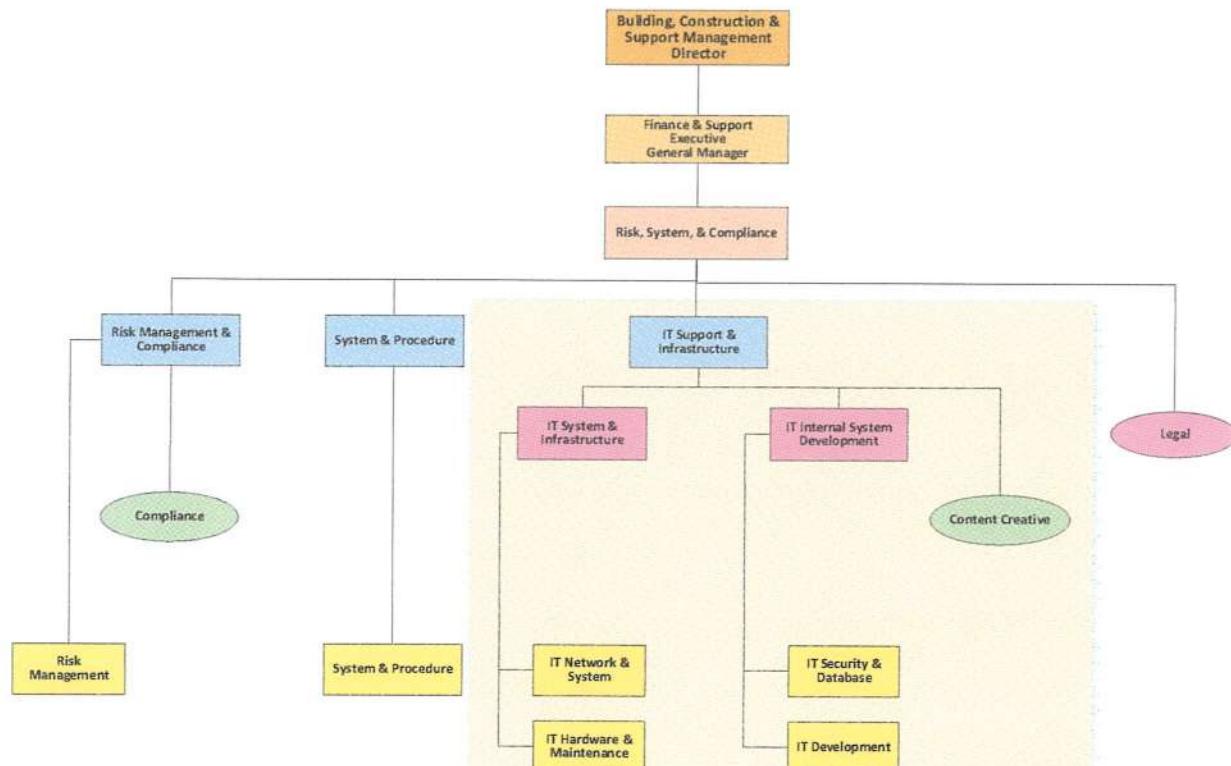
XMMS, Realplayer, PowerDVD, dll.

14. *Software Jaringan* Aplikasi : Perangkat lunak yang digunakan untuk operasional di jaringan computer yaitu browser, *email* dan *chatting*, misalnya Internet Explorer (Google Chrome, Mozilla FireFox, Nestcape, mIRC, Outlook, Outlook Express, dll).
15. *Software Internal* Aplikasi : Perangkat lunak yang dibangun dengan menggunakan *software tools* yang digunakan untuk operasional proses bisnis perusahaan, misalnya *e-procurement*, *preventif maintenance* mesin, bangunan, infrastuktur, *inventory*, SDM, manajemen dokumen, dll.
16. *Server* : Perangkat keras dan perangkat lunak yang berada dalam satu lokasi tertentu untuk diakses oleh komputer dari tempat lain.
17. Sistem Analis : Pegawai yang ditunjuk dan diberi wewenang oleh perusahaan untuk sistem informasi berbasis teknologi informasi.
18. Serangan Siber Segala bentuk perbuatan, perkataan, pemikiran baik yang dilakukan dengan sengaja maupun tidak sengaja oleh pihak manapun, dengan motif dan tujuan apa pun, yang dilakukan di lokasi manapun, yang disasarkan pada sistem elektronik atau muatannya (informasi) maupun peralatan yang sangat bergantung pada teknologi dan jaringan dalam skala apa pun, terhadap obyek vital maupun non-vital dalam lingkup militer dan non-militer, yang mengancam kedaulatan negara, keutuhan wilayah dan keselamatan bangsa.
19. Teknologi Informasi : Seperangkat sistem yang meliputi *hardware* (perangkat keras), *software* (perangkat lunak), dan jaringan komputer untuk mencatat, memproses, menyimpan, dan menyebarkan informasi.
20. *User* : Pengguna komputer/ pegawai atau pihak lain yang diberi hak akses ke dalam jaringan teknologi informasi.

A. Organisasi Satuan Kerja IT

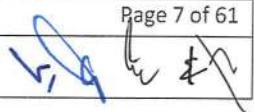
1. Divisi Risk, System & Compliance (RSC) adalah Divisi yang mengelola hal-hal sebagai berikut:
 - a. Pengelola infrastruktur IT, *Hardware, Server & database Management, software license, internal development*, peralatan komunikasi, perangkat CCTV dan berbagai IT Support lainnya.
 - b. Menjalankan prosedur pengendalian keamanan dan kerahasiaan data dalam jaringan komunikasi & sistem informasi
 - c. Sebagai pengelola inisiatif IT baik yang bersifat baru maupun pengembangan.
2. Satuan Kerja IT Support meliputi seluruh Unit Kerja di lingkungan Perusahaan yang terkait dalam melakukan perencanaan, pelaksanaan, *monitoring* dan evaluasi terhadap penggunaan, dan pengelolaan infrastruktur IT yang digunakan di lingkungan Perusahaan.
3. Lokasi penyelenggaraan operasional bisnis Perusahaan yang menggunakan layanan dan infrastruktur TI yang dikelola oleh Satuan Kerja TI, serta sudah melibatkan Satuan Kerja TI sejak proses perencanaan, pengadaan/pembuatan layanan, dan infrastruktur TI, meliputi namun tidak terbatas pada :
 - a. Kantor Pusat
 - b. Kantor Cabang Building Management
 - c. PT UG Arta (bersifat kerjasama)
4. Wewenang dan Tanggung Jawab Satuan Kerja IT Support mengacu pada Struktur Organisasi dan Tata Kerja Perusahaan yang berlaku.

B. Struktur Organisasi



Satuan Kerja IT Support dibentuk dan ditugaskan untuk melaksanakan proses penggunaan dan pengelolaan Teknologi Informasi yang sesuai dengan kebutuhan bisnis, peraturan yang berlaku di lingkungan Perusahaan dan peraturan perundang-undangan yang berlaku. Satuan Kerja IT Support adalah sebagai berikut:

1. Satuan Kerja yang menangani Pengembangan Aplikasi internal:
 - a. Melakukan analisis dan memberikan rekomendasi terkait pengembangan dan pengelolaan aplikasi dalam penyusunan Rencana Strategis TI.
 - b. Menyusun program kerja TI terkait pengembangan dan pengelolaan aplikasi untuk RKAP tahunan yang sejalan dengan Rencana Strategis TI.
 - c. Melakukan penyusunan dan pelaksanaan kebijakan, standar, dan prosedur di bidang pengembangan sistem informasi.
 - d. Melaksanakan pengembangan dan pengelolaan sistem infomasi yang sesuai dengan kebutuhan Rencana Strategis TI.
 - e. Menyiapkan kelengkapan hasil pengembangan, baik *source code* maupun dokumentasi pendukung sebelum proses *deployment*, agar dapat di serahterimakan kepada Satuan Kerja yang Menangani Operasional dan Infrastruktur TI dan dapat di operasionalkan dengan baik.
 - f. Melakukan verifikasi hasil pengembangan aplikasi yang dilakukan vendor (penyedia jasa TI eksternal).
 - g. Menguji dan menjamin kualitas sistem aplikasi TI yang dikembangkan sesuai dengan spesifikasi dan standar kualitas yang ditetapkan.
 - h. Memastikan pelaksanaan program kerja TI terkait pengembangan dan pengelolaan sistem infomasi dapat berjalan sesuai jadwal.
 - i. Melakukan modifikasi perangkat lunak yang ada untuk memperbaiki kesalahan dan penyesuaian dengan perangkat keras baru, untuk meningkatkan *interface* yang menunjang peningkatan kinerja.
 - j. Mengelola terlaksananya proses dan sistem dokumentasi dan administrasi untuk pengembangan aplikasi internal.
2. Satuan Kerja yang menangani Operasional dan Infrastruktur TI
 - a. Menyusun program kerja TI terkait operasional TI untuk RKAP tahunan yang sejalan dengan Rencana Strategis TI.
 - b. Melaksanakan operasional harian semua layanan TI dan infrastruktur pendukungnya, termasuk kegiatan rutin operasional, monitoring, dukungan terhadap permasalahan, dan pengukuran pencapaian tingkat layanan.
 - c. Melakukan pengelolaan insiden dan gangguan layanan yang terjadi, serta melakukan eskalasi jika diperlukan.
 - d. Melakukan pengamanan fisik dan manajemen inventaris atas aset TI yang mengandung informasi penting Perusahaan.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 7 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

- e. Mengelola dan memberikan persetujuan terhadap *Go-Live checklist* untuk menentukan *release* sistem internal (*Deployment* pada aplikasi baru/perubahan, *patching*/ perubahan data, perubahan konfigurasi perangkat).
3. Satuan Kerja yang menangani Keamanan Sistem Informasi TI
 - a. Menyusun dan mengelola desain arsitektur keamanan sistem informasi dan mengajukan *enhancement* yang diperlukan dengan menimbang tren ancaman keamanan sistem informasi terkini.
 - b. Persetujuan terhadap desain, kebijakan, dan prosedur sistem keamanan informasi serta memastikan efektivitas pelaksanaannya.
 - c. Meninjau risiko dan memastikan kepatuhan (*compliance*) yang terkait dengan keamanan informasi terhadap regulasi.
 - d. Memastikan kebijakan, prosedur, dan *awareness* terkait keamanan sistem informasi disosialisasikan kepada seluruh unit kerja terkait di lingkungan Perusahaan.
 - e. Pengelolaan, penanganan, dan pencatatan atas permintaan hak akses, laporan, insiden *Security* terhadap sistem internal.
 - f. Memonitor secara berkala minimal 1 (satu) tahun sekali untuk memastikan tidak ada kelemahan yang dapat mengakibatkan terganggunya operasional TI.
4. Satuan kerja yang menangani Media Sosial

Membuat konten dan mengelola Media Sosial perusahaan sebagai akses penyampaian informasi terkait bisnis dan kegiatan perusahaan kepada masyarakat. Media Sosial yang saat ini digunakan oleh perusahaan adalah sebagai berikut :

- a. *Website*: Menampilkan *profile* perusahaan agar masyarakat dapat mengenal perusahaan lebih dalam serta memperkenalkan produk dan layanan yang ditawarkan.
- b. Aplikasi *messenger (whatsapp)*: Sebagai alternatif komunikasi masyarakat, klien, dan *stakeholder* kepada perusahaan.
- c. *Youtube*: Mengelola publikasi video seperti dokumentasi, arahan, *event-event* perusahaan dan material marketing.
- d. *Instagram*: Mengelola publikasi video konten seperti dokumentasi, arahan, *event-event* perusahaan dan material marketing.

C. Evaluasi Organisasi IT Support

1. Kesesuaian organisasi Satuan Kerja IT Support akan dievaluasi dan diselaraskan dengan kebutuhan Perusahaan mengacu pada Rencana Strategis TI.
2. Pemenuhan formasi SDM TI mengacu pada ketentuan yang ditetapkan oleh HCGA yang meliputi:
 - a. Rekrutmen dan retensi SDM TI yang sejalan dengan kebijakan dan prosedur Perusahaan.
 - b. Pendefinisian dan pemeliharaan *core IT competency* yang dibutuhkan.
 - c. Pemenuhan fungsi di TI (*staffing of roles*).

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 8 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

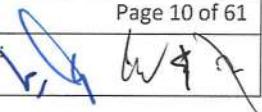
- d. Pelatihan karyawan (mencakup kajian kebutuhan pelatihan dan perencanaannya).
 - e. Ketergantungan terhadap *key individuals* untuk mengurangi risiko misalnya melalui pendokumentasian *knowledge* yang dimiliki, *knowledge sharing, succession planning*, dan penempatan *staff backup*.
 - f. Penilaian kinerja mengakomodir sistem KPI.
 - g. Perubahan dan pemutusan hubungan kerja.
3. Satuan kerja yang menangani strategi, arsitektur, dan perencanaan TI melakukan pemeliharaan dan pemantauan kerangka kerja dan proses organisasi TI.
4. Pemantauan dilakukan setiap adanya penyusunan Rencana Strategis TI (Master Plan TI) yang disertai adanya penambahan maupun pengurangan fungsi organisasi TI, sehingga diperlukan adanya perubahan struktur organisasi menyesuaikan persyaratan *staffing* dan strategi pengadaan untuk memenuhi tujuan bisnis dan perubahan keadaan yang diharapkan.

A. Penyelenggaraan dan Pengelolaan Teknologi Informasi

1. Penyelenggaraan dan pengelolaan *hardware* teknologi informasi meliputi perangkat (*radio/wireless, modem, router, server*, dan jaringan LAN).
2. Penyelenggaraan dan pengelolaan *hardware* teknologi informasi meliputi perangkat (komputer, *printer, scanner, hub LAN, server, modem*).
3. Penyelenggaraan dan pengelolaan *software* berlisensi (*Microsoft, Autocad, dll*) dan teknologi informasi lainnya.
4. Penyelenggaraan analisa dan desain sistem informasi berbasis teknologi informasi.
5. Penyelenggaraan, pengelolaan, dan pemutakhiran *content website ugmandiri.co.id*.
6. Pengelolaan *media sosial* dan aplikasi internal.
7. Dalam hal perencanaan, pengadaan, pembangunan dan pemeriksaan kualitas *hardware, software*, perangkat teknologi informasi yang tergolong spesifik, maka kepada IT Support dapat menggunakan pihak lain (konsultan) yang memiliki kompetensi dan kualifikasi dibidang teknologi informasi apabila diperlukan.

B. Wewenang

1. Dalam hal kegiatan teknologi informasi perusahaan, maka kepada Divisi Risk, System & Compliance cq: IT Support diberi wewenang oleh Direksi untuk:
 - a. Merencanakan dan mengajukan permintaan perangkat atau suku cadang teknologi informasi meliputi perangkat (*radio/wireless link, modem, router, server*, dan jaringan).
 - b. Memberikan rekomendasi teknis/ spesifikasi perangkat untuk digunakan sebelum unit kerja mengajukan permintaan perangkat atau suku cadang teknologi informasi.
 - c. Merencanakan, menentukan, dan mengajukan permintaan pembelian, serta mengecek fisik *software* yang akan dipasang ke dalam komputer/*server* milik perusahaan di setiap Divisi, serta mengajukan audit *software* kepada industri piranti lunak dan piranti keras komersial (*vendor*) resmi maupun badan lain yang ditunjuk oleh vendor tersebut.
 - d. Memastikan setiap perangkat komputer/ laptop telah dipasang/ *install Software* berlisensi seperti Microsoft, Autocad, dll.
 - e. Melakukan aktivasi lisensi *operating System, application System* dan *software*.
 - f. Melakukan pengecekan fisik perangkat teknologi informasi dari proses hasil pengadaan barang maupun kerusakan *hardware* meliputi perangkat (*radio/ wireless link, modem, router, server, dan jaringan*), dan perangkat (komputer, *printer, scanner, switch hub*) yang berlokasi di ruang Direksi.
 - g. Menentukan administrator dari beberapa aplikasi internal guna pengelolaan aplikasi internal dan *databasenya*.
 - h. Membuatkan *email* perusahaan (@ugmandiri.co.id) kepada pegawai.
 - i. Merencanakan dan melakukan konfigurasi jaringan komputer dan penentuan nomor *Internet Protocol (IP)* komputer/ *server* yang terkoneksi ke dalam jaringan teknologi informasi.
 - j. Memberikan hak akses *user* untuk masuk ke dalam jaringan teknologi informasi perusahaan untuk mengakses internet, *email*, dan beberapa aplikasi selain dari hak akses aplikasi internal.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 10 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

- k. Mencari dan mengusulkan konsultan teknologi informasi kepada Direksi untuk perencanaan, pengadaan, pembangunan dan pemeriksaan kualitas *hardware, software,* dan Teknologi Informasi yang tergolong spesifik.
 - l. Membuat dan mengelola media sosial korporasi sebagai akses penyampaian informasi terkait bisnis dan kegiatan perusahaan kepada masyarakat.
2. Dalam hal kegiatan aplikasi internal, untuk memberikan hak akses *user* aplikasi internal diberikan wewenangnya oleh Direksi kepada petugas yang ditunjuk sebagai administrator aplikasi internal.
 3. Dalam hal kegiatan *website ugmandiri.co.id* maka kepada Divisi Risk, System & Compliance diberi wewenang oleh Direksi untuk:
 - a. Mendesain, merencanakan, membangun *website ugmandiri.co.id*.
 - b. Menginput, memperbaiki, meng-update berita-berita ataupun *content website ugmandiri.id* yang pantas dan sesuai untuk dipublikasikan kepada pihak lain.

C. Tanggung Jawab

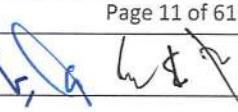
1. Penyelenggaraan dan pengelolaan *hardware* teknologi informasi meliputi perangkat (*modem, router, server, dan jaringan*).
2. Penyelenggaraan dan pengelolaan *hardware* teknologi informasi meliputi perangkat (*komputer, printer, scanner, switch hub*).
3. Penyelenggaraan dan pengelolaan *software* teknologi Informasi.
4. Penyelenggaraan analisa dan desain sistem informasi berbasis teknologi informasi.
5. Batasan hak akses yang diberikan kepada *user* aplikasi internal dalam melakukan kegiatan aplikasi internal, menjadi tanggung jawab administrator aplikasi internal yang ditunjuk.
6. Kebenaran berita-berita, data dan informasi dalam *content website*.
7. Kebenaran dan keabsahan data dan informasi aplikasi internal.

D. Pegawai/User

Pegawai yang berhak memperoleh fasilitas komputer adalah Pegawai/ *user* yang dalam proses pekerjaannya diharuskan menggunakan komputer, maka kepada Pegawai/ *user* tersebut diberikan komputer oleh perusahaan, antara lain Pegawai/ *user* yang bertugas sebagai operator internal, *programmer*, sistem analis, administrator, dan Pegawai/ *user* yang termasuk dalam sistem administrasi yang harus melalui komputer karena adanya aplikasi internal di bidangnya.

E. Komputer dan Hak Akses

1. Pegawai yang berhak mendapat hak akses internet dan *email*.
 - a. Pegawai/ *user* yang dalam proses pekerjaannya menggunakan komputer akan diberikan hak akses jaringan komunikasi komputer perusahaan untuk ke mengakses internet dan *email*.
 - b. Bagi pegawai/ *user* yang memiliki komputer pribadi dan dipakai untuk membantu proses kerjanya di perusahaan, maka kepada pegawai/*user* dan komputernya tersebut diberikan

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi		Halaman :	Page 11 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh:
Tgl Berlaku :	27 Januari 2023	Revisi :	

hak akses jaringan komunikasi komputer perusahaan untuk mengakses internet dan *email*.

2. Pegawai yang berhak mendapat hak akses aplikasi internal

Komputer dan Pegawai/*user* sebagai operator dari suatu aplikasi internal, yang harus mengakses aplikasi internal untuk melaksanakan kegiatannya, maka kepada komputer dan pegawai/*user* tersebut diberi hak akses oleh administrator untuk mengakses aplikasi internal.

F. Aset Perusahaan

1. Komputer yang diberikan kepada Pegawai/*user* yang karena pekerjaanya mengharuskan menggunakan komputer, maka komputer tersebut merupakan aset milik perusahaan.
2. Program aplikasi internal yang dibangun sendiri oleh pegawai atau dibeli dari pihak lain, merupakan aset milik perusahaan.

G. Keamanan Server

1. Semua *server* harus menerapkan sistem registrasi *user* melalui *username* dan *password*.
2. *Password* harus terenkripsi menggunakan metode enkripsi standar.
3. Data yang terdapat pada *server* akan di *back-up* dalam jangka waktu tertentu oleh petugas yang ditunjuk sebagai administrator *database*.

H. Keamanan Hardware

1. *Hardware* yang merupakan sambungan jaringan komunikasi vital antara lain: *modem, switch hub, router*, harus berada dalam suatu ruangan khusus.
2. Ruangan tempat peralatan vital perangkat teknologi informasi sebagaimana dimaksud pada huruf 1, dilengkapi dengan pengaman jaringan listrik bila terjadi hubungan arus pendek, sensor kebakaran, pendingin ruangan (*air conditioner*), alat pemadam kebakaran.
3. Ruangan tempat peralatan vital perangkat teknologi informasi sebagaimana dimaksud pada huruf 1, tidak diperkenankan dimasuki oleh orang lain, selain petugas teknologi informasi atau kecuali telah mendapatkan ijin dari bagian teknologi informasi.

I. Keamanan Cloud Storage

Perusahaan menggunakan *Cloud Storage* bekerjasama dengan pihak ke-3 dalam mengelola *database* perusahaan. Apabila terjadi bencana (*disasater*) maka tahapan yang dilakukan adalah sebagai berikut:

1. *Main Server Disaster*

Auto switch ke *server backup 1* pada saat *disaster*, setelah kerusakan *main server* telah diperbaiki, maka akan kembali/ *auto switch* ke *main server*.

2. *Total Disaster (Main Server & Backup Server 1)*

Restore manual dari *backup server*, setelah kerusakan *main server* telah diperbaiki, maka akan kembali/ *auto switch* ke *main server*.

J. Keamanan Jaringan Komunikasi Komputer dan Aplikasi Internal

1. Untuk memastikan keamanan jaringan komunikasi komputer dan aplikasi internal, maka jalur akses, identifikasi *user*, harus dapat dikontrol oleh administrator jaringan komputer dan database.
2. *Link* komunikasi ke luar dari luar perusahaan diawasi oleh IT Support dengan menggunakan aplikasi berlisensi resmi (Microsoft teams/ Zoom).
3. Pemakaian *Wi-Fi* di lingkungan perusahaan dikelola dan diawasi oleh IT Support dengan menggunakan *provider* yang kredibel.

K. Ketentuan Aplikasi Internal Perusahaan

1. Aplikasi internal yang dibangun baik secara sendiri oleh pegawai ataupun dibeli dari pihak lain untuk keperluan proses bisnis perusahaan, diprioritaskan berbasis *online* dan memperhatikan integrasi dengan aplikasi internal yang sudah berjalan/ada serta memiliki pengamanan data dan informasi, dari gangguan orang-orang yang tidak bertanggung jawab.
2. Apabila aplikasi internal yang karena secara teknis tidak dapat diusahakan memenuhi ketentuan poin 1 di atas, maka hal ini dimungkinkan untuk tidak digunakan di perusahaan.

L. Larangan Pegawai/*user*

1. Selain administrator dan petugas urusan teknologi informasi bagian IT Support, kepada pegawai/*user* dilarang melakukan perubahan/menambah *setting IP* dan nama komputer serta *software* yang telah terpasang di komputer perusahaan.
2. Kepada seluruh pegawai/*user* dilarang melakukan berbagai kegiatan yang melanggar hukum pada saat menggunakan jaringan teknologi informasi perusahaan.
3. Kepada seluruh pegawai/*user* dilarang melakukan kegiatan yang dapat merusak dan menghapus data dan informasi perusahaan dan menyebarkan informasi perusahaan kepada pihak lain.
4. Memberikan *username* dan *password* atau hak akses kepada orang/pihak lain.
5. Mengembangkan/menambah jaringan teknologi informasi tanpa ijin dari Divisi RSC.
6. Menggunakan aset teknologi informasi milik perusahaan, untuk kepentingan pribadi dan atau mendapat keuntungan pribadi.

M. Sanksi

Kepada pegawai/*user* yang terbukti secara sah melakukan kegiatan sebagaimana dimaksud pada larangan di atas, maka kepada pegawai/*user* tersebut dapat dilaporkan kepada pihak berwajib untuk diproses secara hukum sesuai dengan ketentuan/hukum yang berlaku.

Serangan Siber bertujuan untuk merusak atau mendapatkan kontrol atau akses ke dokumen dan sistem penting dalam jaringan komputer bisnis atau pribadi serta didistribusikan oleh individu atau organisasi untuk tujuan politik, kriminal, atau pribadi guna menghancurkan atau mendapatkan akses ke informasi rahasia.

A. Jenis Ancaman Siber

1. Ancaman Perangkat Keras (*hardware threat*)

Ancaman yang disebabkan oleh pemasangan peralatan tertentu yang berfungsi untuk melakukan kegiatan tertentu dalam suatu sistem, sehingga peralatan tersebut merupakan gangguan terhadap sistem jaringan dan perangkat keras lainnya, contoh : *Jamming* dan *Network Intrusion*.

2. Ancaman Perangkat Lunak (*software threat*)

Ancaman yang disebabkan oleh masuknya *software* tertentu yang berfungsi untuk melakukan kegiatan seperti : Pencurian Informasi (*Information Theft*), Perusakan Informasi / Sistem (*Information / System Destruction*), Manipulasi Informasi (*Information Corruption*) dan lain sebagainya, ke dalam suatu sistem.

3. Ancaman Data/Informasi (*data/information threat*),

Ancaman yang diakibatkan oleh penyebaran data/ informasi tertentu yang bertujuan untuk kepentingan tertentu, seperti yang dilakukan dalam *information warfare* termasuk kegiatan propaganda.

B. Bentuk Ancaman Siber

1. Serangan *Advanced Persistent Threats (APT)*, dan *Distributed Denial of Service (DDoS)*

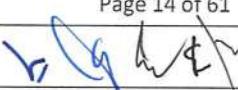
Dilakukan dengan melakukan *overloading* kapasitas sistem dan mencegah pengguna yang sah untuk mengakses dan menggunakan sistem atau sumber daya yang ditargetkan. Serangan ini bertujuan untuk mengganggu operasional sistem, dengan cara menghadapkan sistem pada permintaan akses dan proses yang jauh lebih besar dari yang biasanya ditangani oleh sistem. Sehingga sistem menjadi terlalu sibuk dan *crash*, akibatnya sistem tidak dapat beroperasi dengan maksimal. Permasalahan ini merupakan ancaman yang berbahaya bagi organisasi yang mengandalkan hampir sepenuhnya pada kemampuan internet guna menjalankan roda kegiatannya.

2. Serangan *Defacement*

Dilakukan dengan cara melakukan penggantian atau modifikasi terhadap halaman web sehingga isi dari halaman web berubah sesuai dengan motif penyerang.

3. Serangan *Phishing*

Dilakukan dengan cara memberikan alamat *website* palsu dengan tampilan persis sama dengan *website* aslinya. Tujuan dari serangan *phishing* ini adalah untuk mendapatkan informasi penting dan sensitif seperti *username*, *password* dan lain-lain.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 14 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

4. Serangan *Malware*

Suatu program atau kode berbahaya yang dapat digunakan untuk mengganggu operasi normal dari sebuah sistem komputer. Biasanya program *Malware* telah dirancang untuk mendapatkan keuntungan finansial atau keuntungan lain yang direncanakan. Jumlah serangan *Malware* terus berkembang, sehingga saat ini telah menjadi pandemi yang sangat nyata. *Malware* telah terjadi dimana-mana dan mempengaruhi semua orang yang terlibat dalam setiap sektor kegiatan. Istilah virus generik digunakan untuk merujuk setiap program komputer berbahaya yang mampu mereproduksi dan menyebarkan dirinya sendiri.

5. Serangan *Spam*

Pengiriman *e-mail* secara massal yang tidak dikehendaki, dengan tujuan :

- a. Komersial atau publisitas.
- b. Memperkenalkan perangkat lunak berbahaya, seperti *Malware* dan *crimeware* ke dalam sistem.
- c. Pada situasi terburuk, *spam* menyerupai serangan bom *e-mail*, yang akan berakibat *mail server* mengalami kelebihan beban, *mailbox user* penuh dan ketidaknyamanan dalam pengelolaan.

6. *Social Engineering*

Serangan ini dapat dilakukan dengan menggabungkan serangan lainnya untuk membuat korban mengeklik tautan, mengunduh perangkat lunak jahat, atau mempercayai sumber atau situs berbahaya.

7. Kebocoran Data

Kebocoran data dapat diartikan sebagai transmisi data yang tidak sah dari dalam suatu organisasi ke tujuan atau penerima eksternal. Istilah tersebut dapat digunakan untuk menggambarkan data yang ditransfer secara elektronik atau fisik.

8. *Hacking*

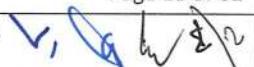
Hacking adalah kegiatan menerobos program komputer milik pihak lain. Biasanya, *hacker* akan mengambil alih sistem jaringan, akun sosial media, akun perbankan, mencuri data, dan lainnya.

9. *Cross-Site Scripting (XSS)*

Sebuah jenis injeksi berupa *script* berbahaya yang diinjeksikan ke sebuah situs rentan maupun terpercaya. *Script* ini dapat mengakses *cookie*, *session token*, ataupun informasi sensitif lainnya yang disimpan *browser*.

10. *SQL Injection*

Jenis injeksi berupa perintah *SQL (Standard Query Language)* yang diinjeksikan ke dalam *data-plane* input untuk mempengaruhi eksekusi *SQL command* yang telah ditentukan.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 15 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

11. Clickjacking

Jenis serangan pada aplikasi web yang membuat korban secara tidak sengaja mengklik elemen halaman web. Klik ini dapat mengaktifkan fungsi jahat yang telah dibuat oleh penyerang, mulai dari arahan mengikuti akun media sosial hingga mengambil uang dari akun bank pengguna.

12. DoS (Denial of Service)

DoS adalah *cyberattack* yang berusaha melumpuhkan sebuah *website* sehingga tidak bisa diakses oleh pengguna. Serangan yang bertubi-tubi tersebut dilakukan oleh para *hacker* agar pertama situs menjadi *down*. Semakin gencar serangannya, maka bisa dipastikan lambat laun *website* menjadi lumpuh total.

13. Credential Reuse

Jenis *cyberattack* yang menyasar data *username*, *password* dan PIN yang mirip atau sama di beberapa akun, maka itu menjadi ancaman serangan dari *Credential Reuse*.

14. Man in the Middle

Sesuai dengan namanya, *cyberattack* jenis ini menempatkan *hacker* di tengah-tengah komunikasi antara dua orang. Ketika Anda sedang berkomunikasi, maka berbagai informasi penting yang dibagikan di antara keduanya bisa dicuri oleh *hacker*.

15. Insider Threat

Ancaman yang berasal dari orang-orang di dalam organisasi, seperti karyawan, mantan karyawan, atau rekan bisnis, yang memiliki informasi orang dalam mengenai praktik keamanan, data, dan sistem komputer organisasi. Sebagai contoh ketika Divisi Finance memiliki *database* karyawan dan Divisi lain mencoba untuk mengaksesnya, maka hal tersebut sangat berisiko untuk mengalami kebocoran data internal.

C. Penanggulangan Serangan Siber

Kegiatan penanggulangan serangan siber dikoordinasikan oleh Divisi RSC dengan menggunakan pendekatan yang menyesuaikan diri dengan sumber dan bentuk serangan yang dihadapi. Bentuk penanggulangan serangan siber yang dilakukan dapat berupa :

1. Pertahanan siber (*cyber defense*),

Suatu upaya untuk menanggulangi serangan siber yang menyebabkan terjadinya gangguan pada terhadap perusahaan. Pertahanan siber disiapkan sebagai suatu upaya penanggulangan serangan siber semacam ini. Tahapan pertahanan siber dapat berupa:

a. Penerapan *Firewall* atau tembok api sebagai sebuah pembatas antara suatu jaringan lokal dengan jaringan lainnya yang sifatnya publik agar setiap data yang masuk dapat diidentifikasi untuk dilakukan penyaringan sehingga aliran data dapat dikendalikan untuk mencegah bahaya/ancaman yang datang dari jaringan publik.

b. Isolasi serangan dengan dukungan implementasi yang efektif dari arsitektur pengamanan tingkat tinggi yang telah ditetapkan, guna mengurangi dampak yang ditimbulkan.

c. Pencarian *Malware* dengan menemukan *backdoor*, *trojan* dan *Malware* lainnya agar tidak menjadi potensi ancaman dikemudian hari.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 16 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh	
Tgl Berlaku :	27 Januari 2023	Revisi :		

- d. Memperbaiki sistem dan data yang telah diserang.
 - e. Melakukan pemulihan sistem dan data ketika terjadi bencana.
 - f. *Disaster Recovery* antara lain menggunakan teknologi *Storage Area Networks (SAN)* dan *Network Attached Storage (NAS)*, untuk *recovery* jika kehilangan data akibat serangan siber.
2. Penanganan secara hukum.

Melakukan koordinasi dengan aparat keamanan terkait apabila telah diketahui pelaku kejahatan siber.

3. Serangan balik siber (*Cyber counter-attack*)

Serangan balik merupakan suatu pilihan yang harus dipertimbangkan secara matang baik dari sisi hukum dan diplomasi. Beberapa contoh serangan balik yang dapat dilakukan oleh tim khusus, antara lain peretasan, penanaman *Malware*, perusakan sistem dan rekayasa kondisi. Tindakan serangan balik terhadap sumber serangan dengan tujuan memberikan efek jera terhadap pelaku serangan siber.

D. Pengelolaan Ancaman

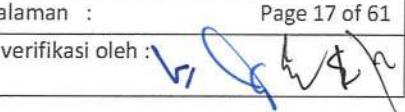
1. Ancaman Terknologi Informasi

terdapat beberapa macam hambatan umum terhadap data dan sistem teknologi informasi yaitu antara lain : Kerusakan perangkat keras dan perangkat lunak, Malware (Malicious Software), Virus computer, Spam, scams, and phishing dan Kesalahan manusia (human error). Selain hambatan umum tersebut, dalam Teknologi Informasi juga mengelola hambatan kriminal terhadap teknologi informasi suatu perusahaan, antara lain yaitu :

- a. Hackers, orang yang menerobos (tidak sah) masuk ke dalam sistem komputer.
- b. Fraud, penggunaan komputer untuk memanipulasi data untuk kepentingan yang melanggar hukum.
- c. Denial of service, serangan online yang membuat pengguna tidak dapat mengakses situs tertentu.
- d. Staff dishonesty, pencurian data/ informasi penting oleh karyawan internal perusahaan.

2. Pengelolaan Ancaman Teknologi Informasi

- a. Mengidentifikasi Risiko, Perusahaan mengungkap, mengenali dan menggambarkan risiko yang mungkin mempengaruhi proyek.
- b. Menganalisis Risiko, Ketika risiko sudah diidentifikasi, perusahaan menentukan kemungkinan dan konsekuensi dari setiap risiko yang ada. Perusahaan lalu mengembangkan sebuah pemahaman tentang sifat risiko dan potensi untuk mempengaruhi tujuan dan sasaran proyek .
- c. Mengevaluasi Risiko, Perusahaan mengevaluasi risiko dengan menentukan besarnya risiko, yang merupakan kombinasi dari kemungkinan dan konsekuensi. Lalu perusahaan membuat keputusan apakah risiko itu dapat diterima atau tidak.
- d. Memantau dan Mempertimbangkan Risiko, Ini adalah proses dimana perusahaan memantau setiap risiko yang ada untuk menghindari risiko yang lebih besar.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi		Halaman :	Page 17 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh : 
Tgl Berlaku :	27 Januari 2023	Revisi :	

Standar Prosedur Operasional Pengelolaan Teknologi Informasi (TI) Bab V Fungsi Teknologi Informasi	 <i>serve you better</i>
---	--

A. Ketentuan IT Security Policy

IT *Security Policy* merupakan penerapan *Security* dari point-point Pengelolaan Teknologi Informasi (IT Policy). **IT Security Policy** dirumuskan oleh Unit kerja IT dan disepakati oleh seluruh Unit Kerja lainnya. Faktor yang dipertimbangkan termasuk pengguna (*user*) dan bisnis perusahaan. Adapun beberapa kebijakan yang dibuat meliputi:

1. Kebijakan tentang perawatan *System*

Kebijakan Tentang Perawatan Sistem Kebijakan perawatan sistem diperlukan untuk memaksimalkan perawatan terhadap sistem yang berjalan, Kebijakan perawatan sistem Perusahaan meliputi:

- a. Memastikan bahwa sistem informasi yang diimplementasikan berjalan dengan baik.
- b. Penerapan kebijakan ini diperuntukkan kepada pemangku kepentingan dan pegawai yang berkepentingan di bagian Teknologi Informasi dan juga pihak ketiga yang menjadi vendor.
- c. Perawatan sistem harus sesuai dengan pedoman yang berlaku.
- d. Membuat prosedur-prosedur yang berkaitan dengan perawatan sistem yang meliputi perawatan korektif, perawatan adaptif, perawatan prefektif dan perawatan preventif.
- e. Monitoring diperlukan untuk memantau semua kegiatan yang berhubungan dengan perawatan *System* Perusahaan.

2. Kebijakan Penanganan Risiko

Kebijakan penanganan risiko diperlukan untuk menangani risiko-risiko yang mungkin ada pada saat implementasi sistem. Kebijakan penanganan risiko Perusahaan meliputi:

- a. Mengidentifikasi dan menganalisis kemungkinan risiko yang ada pada implementasi sistem informasi diperusahaan.
- b. Penerapan kebijakan ini diperuntukkan kepada semua pegawai di lingkungan perusahaan yang berhubungan dengan Aset informasi.
- c. Penanganan risiko terhadap sistem dan aset informasi yang berjalan harus sesuai dengan pedoman yang berlaku.
- d. Membuat prosedur-prosedur yang berkaitan dengan manajemen risiko yang meliputi mengembangkan kriteria pengukuran risiko, mengembangkan profil Aset informasi, mengidentifikasi container dari aset informasi, mengidentifikasi area masalah, mengidentifikasi skenario ancaman, mengidentifikasi risiko, menganalisis risiko, dan memilih pendekatan pemilihan pemilihan penanganan risiko.
- e. Monitoring diperlukan untuk memantau semua kegiatan yang berhubungan dengan penanganan risiko Perusahaan.

3. Kebijakan Sumber Daya Manusia Pengaturan Hak Akses

Kebijakan sumber daya manusia dan pengaturan hak akses diperlukan untuk mengatur batasan-batasan dari pengguna sistem informasi di lingkungan Perusahaan. Kebijakan sumber daya manusia dan pengaturan hak akses perusahaan meliputi:

- a. Mengendalikan akses pengguna sistem informasi dengan mengatur hak akses pengguna. Tujuan lainnya sebagai upaya pengurangan risiko dari penyalahgunaan fungsi atau wewenang akibat kesalahan manusia.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 18 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

- b. Penerapan kebijakan ini diperuntukkan kepada pemangku kepentingan dan pimpinan perusahaan untuk menentukan atau mengelola penentuan sumber daya manusia dengan pengaturan hak akses terhadap sistem.
- c. Penetuan pengaturan hak akses terhadap sistem harus sesuai dengan pedoman dan aturan yang berlaku dilingkungan Perusahaan. Disesuaikan juga dengan kemampuan sistem informasi mengelola hak akses
- d. Membuat prosedur-prosedur yang berkaitan dengan pengaturan hak akses yang meliputi permintaan akses, pemberian akses, pemantauan identitas pengguna, penilaian kinerja pegawai, perilaku kerja pegawai, pembatasan akses, penghapusan akses, permasalahan akses dan pencatatan akses.
- e. Monitoring diperlukan untuk memantau semua kegiatan yang berhubungan dengan pengelolaan sumber daya manusia dan pengaturan hak akses sistem infromasi di Perusahaan.

4. Kebijakan Keamanan dan Pengendalian Aset Informasi

Kebijakan keamanan dan pengendalian aset diperlukan untuk mengatur dan mengelola aset informasi perusahaan. Kebijakan keamanan dan pengendalian aset informasi perusahaan meliputi:

- a. Memberikan perlindungan terhadap aset perusahaan berdasarkan tangkat perlindungan yang diberikan.
- b. Penerapan kebijakan ini diperuntukkan kepada pemangku kepentingan dan pimpinan perusahaan beserta seluruh pegawai terhadap keamanan aset informasi dalam penggunaan sistem informasi.
- c. Pedoman keamanan dan pengendalian Aset informasi di lingkungan perusahaan harus disesuaikan dengan aturan-aturan yang berlaku baik aturan dari sistem informasi maupun aturan dari perusahaan.
- d. Membuat prosedur-prosedur yang berkaitan dengan keamanan aset dan pengendalian aset informasi meliputi klasifikasi informasi dan tanggungjawab informasi.
- e. Monitoring diperlukan untuk memantau semua kegiatan yang berhubungan dengan pengendalian aset informasi sistem informasi di Perusahaan.

5. Kebijakan Keamanan Server

Kebijakan lain yang harus diperhatikan oleh perusahaan adalah kebijakan keamanan *server*. Kebijakan ini diperlukan untuk memaksimalkan keamanan terhadap *server* data yang secara langsung juga akan menjaga kerahasiaan data Perusahaan dan data privasi karyawan Perusahaan terhadap kejadian komputer yang akan merugikan Perusahaan. Kebijakan Keamanan *Server* Perusahaan meliputi:

- a. Memaksimalkan keamanan sistem informasi Perusahaan dari *server* yang digunakan.
- b. Penerapan kebijakan ini diperuntukkan kepada pemangku kepentingan dan pegawai yang berkepentingan di bagian Teknologi Informasi.
- c. Konfigurasi *server* harus sesuai dengan pedoman yang berlaku.

- d. Membuat prosedur-prosedur yang berkaitan dengan keamanan *server* meliputi: prosedur pembuatan *server* sendiri, prosedur penyimpanan *server*, prosedur keamanan ruangan *server*, penjaga *server*, dan penggunaan sever.
- e. Monitoring diperlukan untuk memantau semua kegiatan yang berhubungan dengan keamanan *server* Perusahaan.

B. Ketentuan Pengembangan Sistem

Pengembangan sistem merupakan penyusunan suatu sistem yang baru untuk menggantikan sistem yang lama secara keseluruhan atau memperbaiki sistem yang telah ada.

1. Pengembangan Sistem

Sistem lama yang perlu diperbaiki atau diganti disebabkan karena beberapa hal :

- a. Adanya permasalahan-permasalahan (problems) yang timbul di sistem yang lama. Permasalahan yang timbul dapat berupa :

1) Ketidakberesan sistem yang lama

Ketidakberesan dalam sistem yang lama menyebabkan sistem yang lama tidak dapat beroperasi sesuai dengan yang diharapkan.

2) Pertumbuhan organisasi

Kebutuhan informasi yang semakin luas, volume pengolahan data semakin meningkat, perubahan prinsip layanan akademik yang baru menyebabkan harus disusunnya sistem yang baru, karena sistem yang lama tidak efektif lagi dan tidak dapat memenuhi lagi semua kebutuhan informasi yang dibutuhkan pengguna sistem informasi.

b. Untuk memanfaatkan peluang pasar

Dalam keadaan persaingan pasar yang ketat, kecepatan informasi atau efisiensi waktu sangat menentukan berhasil atau tidaknya strategi dan rencana-rencana yang telah disusun untuk memanfaatkan peluang pasar sebanyak banyaknya, sehingga teknologi informasi perlu digunakan untuk meningkatkan penyediaan informasi agar dapat mendukung proses pengambilan keputusan yang dilakukan oleh Manajemen.

- c. Adanya instruksi dari pimpinan atau adanya peraturan pemerintah Penyusunan sistem yang baru dapat juga terjadi karena adanya instruksi-instruksi dari atas pimpinan ataupun dari luar organisasi, seperti misalnya peraturan pemerintah.

2. Indikator Diperlukannya Pengembangan Sistem

- a. Keluhan pengguna
- b. Pembayaran gaji yang tidak sesuai
- c. Laporan yang tidak tepat waktu
- d. Isi laporan yang sering salah
- e. Tanggung jawab yang tidak jelas
- f. Kegiatan yang tumpang tindih
- g. Tanggapan yang lambat terhadap gangguan

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 20 of 61
No Reg.:	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

- h. Kehilangan kesempatan kompetisi dengan perusahaan lain
 - i. Ketersediaan sistem informasi yang kurang
 - j. *File-file* yang kurang teratur
3. Dengan adanya sistem baru diharapkan terjadi peningkatan dalam hal :
- a. Kinerja, yang dapat diukur dari *throughput* dan *respon time*.
Throughput : jumlah pekerjaan yang dapat dilakukan pada suatu saat tertentu.
Respon time : Rata-rata waktu tertunda di antara dua transaksi.
 - b. Kualitas informasi yang disajikan.
 - c. Keuntungan (penurunan biaya). Berhubungan dengan jumlah sumber daya yang digunakan.
 - d. Kontrol (pengendalian).
 - e. Efisiensi.
 - f. Pelayanan.
4. Prinsip Pengembangan Sistem
- Prinsip-prinsip pengembangan sistem, adalah :
- a. Sistem yang dikembangkan adalah untuk pengguna di dalam dan luar Perusahaan.
 - b. Sistem yang dikembangkan adalah investasi modal yang besar
- Maka setiap investasi modal harus mempertimbangkan 2 hal berikut ini :
- 1) Semua alternatif yang ada harus diinvestigasikan
 - 2) Investasi yang terbaik harus bernilai
 - c. Sistem yang dikembangkan memerlukan orang yang terdidik
 - d. Tahapan kerja dan tugas-tugas yang baru dilakukan dalam proses pengembangan sistem
 - e. Proses pengembangan sistem tidak harus urut
 - f. Dokumentasi harus ada untuk pedoman dalam pengembangan sistem

C. Ketentuan *log* dan Pemantauan

File log dikenali sebagai *file* yang sering dicap waktu yang secara virtual dapat merekam semua informasi penting tentang peristiwa yang terjadi dalam lingkup jaringan TI, OS, atau aplikasi perangkat lunak lainnya. Beberapa *file log* dapat diinterpretasikan secara manusiawi, sementara yang lain sebagian besar dimaksudkan untuk digunakan oleh mesin. Dengan spektrum kasus penggunaan yang luas, *file log* sering dikategorikan ke dalam *log audit*, *log transaksi*, *pelanggan*, *log*, *log pesan*, *log* untuk kesalahan atau peristiwa, dan sebagainya.

File log dapat mengurangi waktu tunggu yang dibutuhkan untuk mengumpulkan wawasan tentang suatu peristiwa dan membuat proses *Root Cause Analysis* (RCA) lebih efisien. Meskipun nilai *file log* tidak terbantahkan, mengekstraksi nilai itu menjadi tantangan karena skala biaya. Jaringan dan platform yang memproses *file log* tingkat tinggi dapat membelokkan proporsi yang signifikan

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 21 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

dari keseluruhan anggaran dan membuat perbedaan dalam biaya ini karena *throughput file log* tidak konsisten. Bahkan setelah menimbulkan biaya, mungkin mendapatkan *file log* yang membawa nilai istimewa dalam kasus penggunaan yang sangat spesifik.

Merumuskan dan menerapkan kebijakan manajemen *log* dapat mengoptimalkan alokasi sumber daya di seluruh jaringan TI. Di luar itu, ada dimensi yang terdefinisi dengan baik di mana gagasan manajemen *log* bersandar. Satu dimensi berfokus pada sifat eksplorasi di mana kerentanan antara perangkat yang terhubung, *platform cloud*, dan sistem terdistribusi dapat difilter dan ditandai tepat waktu.

Dimensi lainnya berfokus pada penajaman kinerja jaringan dengan memastikan waktu aktif yang konsisten. Untuk mencapai tujuan keamanan dan keandalan sistem ini, profesional manajemen jaringan TI memerlukan kebijakan manajemen *log* yang bijaksana. Kebijakan Manajemen *log* dan pemantauan meliputi:

1. *Log File Forwarders* ke Manajemen *log* Terpusat

Pengalih *log* harus menjadi unit pusat sistem manajemen *log*. Ini akan memberi tim kendali yang lebih besar, aksesibilitas yang lebih mudah, dan perspektif untuk mengoptimalkan *file log* sesuai anggaran yang dialokasikan dengan menangani *throughput*.

Pada sistem operasi ini, aplikasi perusahaan akan menghasilkan *file log* di sistem lokal, dan penerus akan memperluas *file log* untuk melakukan analitik. Semua kompresi terjadi di tingkat penerusan dengan kemampuannya untuk mengirim ulang *file*. Ini membebaskan ruang untuk aplikasi inti untuk beroperasi di lingkungan yang tidak terganggu namun terkelola.

Pengalih *file log* yang sama dapat bertindak sebagai solusi cadangan jika terjadi kegagalan sistemik. Jika sistem rusak, segera setelah dimulai ulang, penerusan dapat mengirim *file*. Ini mengurangi ketergantungan pada waktu aktif sistem untuk mengirim *file log* penting.

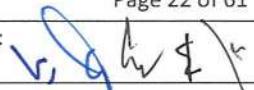
a. Membuat panduan Akses dan Notifikasi

Sebagian besar *file log* berada di bawah dua kategori proses *logging* yang bertanggung jawab untuk mengirim entri dan yang lainnya bertanggung jawab untuk menarik keluar entri. Saat entri *log* dikirim, harus ada panduan yang ditetapkan tentang tingkat *logging* yang tersedia dan tingkat apa yang sesuai untuk kasus penggunaan apa.

Mengirimkan informasi dalam jumlah besar dapat mengakibatkan gangguan data dan konsumsi sumber daya yang kurang optimal. Jadi, di sisi penerima data *logging*, keamanan sistem dan operasi TI mengambil posisi yang diinginkan. Otorisasi data sensitif di *file log* dapat disalahgunakan untuk menimbulkan ancaman bagi seluruh sistem. Karenanya, kebijakan *log* pada notifikasi harus berfokus sepenuhnya pada satu pertanyaan - siapa yang diberi tahu tentang apa, kapan, dan bagaimana

b. Memastikan Kepatuhan untuk Pengumpulan Data *log*

Data *log* harus mengumpulkan informasi dengan cara yang memenuhi pedoman yang ditetapkan berdasarkan PCI DSS, FISMA, SOX, HIPAA, dan kebijakan lain yang relevan dengan persyaratan bisnis yang ditentukan. Laporan yang memerlukan informasi yang menunjukkan kepatuhan harus dibuat dengan mudah.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 22 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

c. Penyimpanan Data *log* Tanpa Batas

Memfilter data *log* pada tahap awal dapat menjadi tidak efisien dari segi biaya dan proses karena tidak ada indikator penting yang menunjukkan *file log* mana yang akan dapat digunakan untuk tantangan TI yang diberikan. Platform harus direkayasa untuk mengatasi masalah ini dengan memungkinkan dapat menyimpan terabyte data *log* setiap hari. Setelah perusahaan memiliki data di satu tempat, maka dapat membuat aturan pengindeksan untuk memprioritaskan *file log* kasus penggunaan dalam perusahaan. Untuk Penyimpanan log firewall dilakukan selama 3 tahun.

d. Platform Manajemen *log* Di kalibrasi untuk Kinerja Optimal

Manajemen *log* Motadata memiliki kemampuan untuk mengumpulkan, menggabungkan, dan mengindeks dengan cerdas semua data *log* apa pun formatnya. Dengan cara ini, perusahaan menyimpan data yang dapat ditafsirkan oleh manusia serta yang dihasilkan oleh mesin, dalam format terstruktur atau tidak terstruktur. Dengan kemampuan Analisis Data yang kaya pada platform yang sama, perusahaan dapat melakukan studi analisis korelasi untuk mengumpulkan laporan secara efisien tentang risiko operasional dan keamanan.

Bersamaan dengan ini, modul *Network Flow Analytics* membantu dalam memantau semua lalu lintas di antara perangkat yang terhubung di jaringan yang mendukung Netflow V5 & V9, sFlow, IPFIX, dan tata letak lainnya. Perusahaan dapat memanfaatkan aliran data ini untuk mengumpulkan wawasan tentang kemacetan di jaringan TI berdasarkan tren lalu lintas dan interaksi kritis antara pengguna atau aplikasi. Perusahaan dapat dengan mudah mematuhi standar kepatuhan tinggi seperti PCI DSS, FISMA, dan HIPAA.

Memanfaatkan kemampuan pengumpulan & agregasi data yang komprehensif, di samping pengindeksan cerdas dan antarmuka pencarian yang lancar, tim TI dalam perusahaan dapat menggunakan Manajemen *log* Motadata untuk secara sistematis mengoptimalkan praktik *file log* di perusahaan sambil tetap mematuhi standar kepatuhan dan efisiensi operasional tertinggi.

Dalam rangka pemeliharaan dan peningkatan logs untuk setiap hardware/ software, setiap melakukan maintenance dan update software maupun upgrade hardware perlu didokumentasikan dengan cara melakukan pencatatan waktu.

D. Ketentuan Insiden Keamanan Informasi

1. Tujuan

Digunakan untuk memperkuat dan meningkatkan kontrol keamanan informasi serta Untuk mengurangi kemungkinan atau konsekuensi dari insiden di masa depan. Perusahaan menetapkan prosedur untuk mengukur dan memantau jenis, volume, dan biaya insiden keamanan informasi. Informasi yang diperoleh dari evaluasi insiden keamanan informasi harus digunakan untuk:

- a. Meningkatkan rencana manajemen insiden termasuk skenario dan prosedur insiden.
- b. Mengidentifikasi insiden yang berulang atau serius dan penyebabnya untuk memperbarui penilaian risiko keamanan informasi organisasi dan menentukan serta menerapkan kontrol tambahan yang diperlukan untuk mengurangi kemungkinan atau konsekuensi dari insiden serupa di masa depan. Mekanisme untuk mengaktifkan

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 23 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

yang mencakup pengumpulan, penghitungan dan pemantauan informasi tentang jenis insiden, volume dan biaya.

- c. Meningkatkan kesadaran dan pelatihan pengguna dengan memberikan contoh tentang apa yang bisa terjadi, bagaimana menanggapi insiden tersebut dan bagaimana menghindarinya di masa depan.

2. Prosedur Manajemen Informasi

Tujuan manajemen insiden keamanan informasi harus disetujui oleh manajemen dan harus dipastikan bahwa mereka yang bertanggung jawab atas manajemen insiden keamanan informasi memahami prioritas organisasi untuk menangani insiden keamanan informasi termasuk kerangka waktu penyelesaian berdasarkan potensi konsekuensi dan tingkat keparahan. Prosedur manajemen insiden harus diterapkan untuk memenuhi tujuan dan prioritas ini.

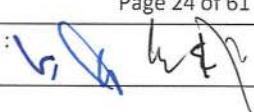
Manajemen harus memastikan bahwa rencana manajemen insiden keamanan informasi dibuat dengan mempertimbangkan skenario dan prosedur yang berbeda dikembangkan dan diimplementasikan untuk aktivitas berikut:

- a. Evaluasi peristiwa keamanan informasi menurut kriteria untuk apa yang merupakan insiden keamanan informasi.
- b. Pemantauan, deteksi, klasifikasi, analisis dan pelaporan peristiwa dan insiden keamanan informasi (dengan cara manusia atau otomatis).
- c. Mengelola insiden keamanan informasi hingga kesimpulan, termasuk respons dan eskalasi, menurut jenis dan kategori insiden, kemungkinan aktivasi manajemen krisis dan aktivasi rencana kesinambungan, pemulihan terkendali dari insiden dan komunikasi ke internal dan pihak luar yang berkepentingan.
- d. Koordinasi dengan pihak berkepentingan internal dan eksternal seperti otoritas, kelompok dan forum kepentingan eksternal, pemasok dan klien.
- e. Penanganan barang bukti.
- f. Analisis akar penyebab atau prosedur post-mortem.
- g. Identifikasi pelajaran yang dipetik dan setiap perbaikan pada prosedur manajemen insiden atau kontrol keamanan informasi secara umum yang diperlukan.

3. Peran dan Tanggung Jawab

Perusahaan menetapkan proses manajemen insiden keamanan informasi yang sesuai. Peran dan tanggung jawab untuk melaksanakan prosedur manajemen insiden ditentukan dan dikomunikasikan secara efektif kepada pihak berkepentingan internal dan eksternal yang relevan dengan mempertimbangkan hal-hal sebagai berikut:

- a. Menetapkan metode umum untuk melaporkan peristiwa keamanan informasi termasuk titik kontak.
- b. Menetapkan proses manajemen insiden untuk menyediakan organisasi dengan kemampuan untuk mengelola insiden keamanan informasi termasuk administrasi, dokumentasi, deteksi, prioritas, analisis, komunikasi dan koordinasi pihak yang berkepentingan.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 24 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

- c. Menetapkan proses respons insiden untuk menyediakan kemampuan bagi Perusahaan untuk menilai, menanggapi, dan belajar dari insiden keamanan informasi.
- d. Hanya mengizinkan personel yang kompeten untuk menangani masalah yang terkait dengan insiden keamanan informasi di dalam Perusahaan. Pegawai tersebut harus dilengkapi dengan dokumentasi prosedur dan pelatihan berkala.
- e. Menetapkan proses untuk mengidentifikasi pelatihan yang diperlukan, sertifikasi dan pengembangan profesional berkelanjutan untuk personel tanggap insiden.

Setiap Respon terhadap insiden perlu dilakukan pengujian terlebih dahulu sebelum diimplementasikan dan didokumentasikan pengujian rencana respon tersebut.

E. Ketentuan Kontrol Akses

Kontrol Akses adalah suatu proses dimana *user* diberikan akses dan hak untuk melihat *System*, sumber atau informasi. Untuk keamanan komputer, kontrol akses meliputi otorisasi, otentikasi, dan audit dari suatu kesatuan untuk memperoleh akses. Kontrol akses memiliki subjek dan objek. *User* (manusia), adalah subjek yang mencoba untuk mendapatkan akses dari objek/ *software*. Dalam sistem komputer, daftar kontrol akses berisi perizinan dan data kemana *user* memberikan izin tersebut. Data yang telah memiliki izin hanya dapat dilihat oleh beberapa orang dan ini tentunya sudah dikontrol oleh kontrol akses. Hal ini memungkinkan administrator untuk mengamankan informasi dan mengatur hak atas informasi apa saja yang boleh diakses, siapa yang bisa mengakses informasi tersebut, dan kapan informasi tersebut bisa diakses.

1. Fungsi kontrol akses

Fungsi kontrol akses yaitu memberikan ijin kepada pengguna yang memiliki hak untuk menggunakan sumber daya yang ada. Dengan demikian, fungsi yang lainnya yaitu mencegah pengguna maupun penyusup yang berusaha menggunakan sumber daya tersebut.

Fungsi kontrol akses ini juga sebagai hak akses untuk ke suatu daerah. Contohnya saja seperti saat kita pergi ke suatu tempat yang penting atau ruang rapat. Tentu banyak macam pengamanan yang akan kita temui sebagai akses *control* sehingga ruang rapat itu sangat penting hanya untuk kegiatan tertentu dan akses perorangannya sangat dibatasi. Hanya hanya orang tertentu yang dapat mengakses ruang rapat tersebut.

2. Cara kerja kontrol akses

Sekali *user log in* ke *System*, maka *user* tersebut diberikan otorisasi untuk mengakses sumber daya sistem. Yang perlu diperhatikan adalah, siapa saja yang boleh membaca isi *file* kita, siapa saja yang boleh merubah isi *file* kita, dan bolehkan *file* kita di-share ke *user* lain.

Terdapat beberapa metode dalam kontrol akses , diantaranya:

- a. Metode Ownership.
- b. Pembuat *file* adalah pemilik *file*.
- c. Id pembuat *file* disimpan.
- d. Hanya pemilik yang dapat mengakses *file* miliknya.
- e. Administrator juga dapat mengaksesnya.
- f. Metode *File Types*.
- g. *File* akan didefinisikan sebagai *public file*, *semipublic file* atau *private file*.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 25 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

**Standar Prosedur Operasional
Pengelolaan Teknologi Informasi (TI)**

Bab V Fungsi Teknologi Informasi



- h. *Public file*, semua user memiliki hak penuh (rwx).
- i. *Semi public file*, user lain hanya mempunyai hak read execute (xr).
- j. *Private file*, user lain tidak punya hak.

3. Akses kontrol terbagi menjadi beberapa model

a. *Mandatory Kontrol Akses (MAC)*

Akses kontrol di mana hak akses diatur oleh pusat berdasarkan tingkat keamanan.

b. *Discretionary Kontrol Akses (DAC)*

Akses kontrol di mana pemilik dari sistem menentukan siapa saja yang diberi hak akses. Dari sistem ini memungkinkan penyebaran hak akses dapat dibatasi.

c. *Role-Based Kontrol Akses (RBAC)*

Akses kontrol di mana hak akses diatur berdasarkan peran di dalam suatu perusahaan atau organisasi tertentu. Misalkan ruangan manajer hanya dapat diakses oleh manajer itu sendiri, sedangkan karyawan tidak dapat mengakses ruangan tersebut.

d. *Attribute-Based Kontrol Akses (ABAC)*

Akses kontrol di mana hak akses diberikan menggunakan atribut dari pengguna. Terdapat 3 aspek utama dari kontrol akses, sebagai berikut:

e. *Authentication*

Melakukan verifikasi bahwa pengguna atau entitas sistem tertentu adalah valid untuk melakukan akses terhadap sistem.

f. *Authorization*

Pemberian hak atau izin terhadap entitas sistem untuk mengakses sumber daya sistem. Fungsi ini menentukan siapa yang dipercaya untuk melakukan aksi tertentu di dalam sistem.

g. *Audit*

Sebuah review independen berupa pemeriksaan catatan dan kegiatan sistem untuk menguji sejauh mana berjalannya mekanisme pengendalian sistem, memastikan kepatuhan terhadap kebijakan dan prosedur operasional yang telah ditetapkan, mendeteksi adanya pelanggaran terhadap prosedur keamanan, dan untuk merekomendasikan perubahan dalam hal kontrol.

4. Kelebihan Kontrol Akses

a. Menghalangi Pencurian

Sebuah akses *control* tentunya membatasi orang yang dapat mengakses ke area-area yang eksklusif. Tentunya area tersebut dikatakan eksklusif karena menyimpan sesuatu yang berharga, tentunya dapat mencegah terjadinya pencurian yang mungkin terjadi.

b. Meningkatkan level sekuritas.

Di jaman sekarang, sekuritas semakin canggih, seperti contohnya saat kita melakukan transaksi, kita mempunyai atm yang harus di masukan PIN terlebih dahulu. Saat masuk hotel ada *tapping* kartu terlebih dahulu.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 26 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

F. Ketentuan IT *continuity*

Kebijakan operasional tata kelola IT meliputi pengelolaan layanan IT, pengelolaan *Security* IT, pengelolaan layanan pihak ketiga, monitor dan evaluasi kinerja IT, monitor dan evaluasi pengendalian internal, serta pengelolaan *compliance external regulation*.

1. Pengelolaan Layanan IT

Merupakan kebijakan yang mengatur tata kelola layanan IT. Kebijakan ini bertujuan agar proses layanan IT dapat teridentifikasi dan mampu didefinisikan dengan baik untuk mencapai kinerja IT yang diharapkan demi kelangsungan layanan IT perusahaan.

Kebijakan pengelolaan Layanan IT dapat dituangkan dalam prosedur atau standar yang mengatur secara lebih detail proses yang diperlukan dalam menyelenggarakan layanan IT. *Best practice* yang dapat digunakan adalah IT *Infrastructure Library* (*ITIL*) dengan penyesuaian yang diperlukan.

2. Pengelolaan Sekuriti IT

Kebijakan ini mengatur tata kelola sekuriti IT dalam perusahaan yang bertujuan untuk menjaga kerahasiaan (*confidentiality*), intergritas (*integrity*), dan ketersediaan (*availability*) informasi perusahaan. Ruang lingkupnya mencakup aspek-aspek tentang pendefinisian aturan *Security* IT, yang meliputi, rencana sekuriti IT, klasifikasi aset IT, prosedur sekuriti, monitoring (pendekripsi, pelaporan, penyelesaian vulnerabilities & insiden sekuriti) dan Rencana kesinambungan bisnis perusahaan atau *Disaster Recovery Plan* (*DRP*).

Kebijakan Pengelolaan Sekuriti IT dapat dituangkan dalam suatu prosedur atau standar sekuriti IT yang pada umumnya mengadopsi proses *Information Security Management System* (*ISMS*) yang berbasis ISO 27000 dan disesuaikan dengan kebutuhan perusahaan.

3. Pengelolaan Layanan Pihak Ketiga

Kebijakan yang mengatur tata kelola layanan IT yang dilakukan oleh pihak ketiga (*outsourcing*). Kebijakan ini bertujuan untuk menjamin bahwa layanan yang dilakukan oleh pihak ketiga (*suppliers, vendors, dan partners*) memenuhi kebutuhan bisnis perusahaan, serta meminimalkan risiko bisnis jika pihak ketiga tidak dapat memenuhi kewajibannya dalam memberikan layanan IT.

Ruang lingkupnya meliputi pendefinisian tugas, tanggung jawab, dan ekspektasi dalam perjanjian dengan pihak ketiga. Kebijakan ini mengatur proses identifikasi hubungan pihak ketiga, *supplier relationship management*, *supplier risk management*, dan *supplier performance monitoring*.

Kebijakan ini dapat berupa prosedur pengelolaan hubungan kemitraan dengan pihak ketiga, prosedur pengelolaan risiko untuk layanan pihak ketiga, prosedur pemantauan kinerja pihak ketiga, serta pembuatan kontrak dengan pihak ketiga berdasarkan persyaratan yang berlaku.

4. Monitor dan Evaluasi Kinerja IT

Kebijakan yang mengatur pengelolaan indikator kinerja IT hingga level korporat dan sistematika pelaporan kinerja serta tindak lanjut yang diperlukan jika terjadi deviasi. Tujuannya untuk memastikan seluruh kinerja IT sesuai dengan arahan dan kebijakan yang berlaku.

Ruang lingkupnya meliputi pengaturan pendekatan dan metoda monitoring kinerja IT, pendefinisian dan cara pengumpulan data, proses asesmen kinerja IT, proses pelaporan

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi	Halaman :	Page 27 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02
Tgl Berlaku :	27 Januari 2023	Revisi :

kinerja IT secara periodik, serta proses perencanaan remediasi akibat deviasi hasil asesmen kinerja IT.

Kebijakan ini dapat dituangkan dalam prosedur pengukuran kinerja yang didefinisikan dalam KPI (*Key Performance Indikator*) unit, prosedur tata cara pengumpulan data kinerja IT, prosedur proses pelaksanaan asesmen kinerja IT, prosedur pelaporan kinerja IT, dan prosedur tata cara remediasi deviasi kinerja IT.

5. Monitor dan Evaluasi Pengendalian Internal

Monitor dan Evaluasi Pengendalian Internal adalah kebijakan yang diperlukan untuk *internal control* (pengendalian internal). Kebijakan ini bertujuan untuk memberikan jaminan mengenai operasi IT yang efektif dan efisien, serta kepatuhannya terhadap kebijakan dan aturan yang berlaku di perusahaan.

Kebijakan ini dapat mengatur proses monitoring dan pelaporan pengecualian *control (control exception)*, pengelolaan asesmen dan hasil dari *control self assessment* (CSA), serta mengelola proses remediasi, dan *review* pihak ketiga. Monitor dan Evaluasi Pengendalian Internal dapat dituangkan ke dalam pendefinisian pengendalian internal yang akan diterapkan dalam layanan IT, prosedur pelaporan pengecualian kontrol, prosedur asesmen dan *control self assessment*, prosedur tata cara remediasi, dan prosedur tata cara mengevaluasi pihak ketiga.

6. Pengelolaan *Compliance External Regulation*

Kebijakan yang mengatur proses identifikasi kebutuhan compliance dan proses evaluasi untuk menjamin *compliance* terhadap aturan yang berlaku. Kebijakan ini ditujukan untuk memastikan bahwa persyaratan aturan atau hukum yang berlaku telah dipatuhi. Ruang lingkupnya dapat mengatur proses identifikasi persyaratan compliance, mengoptimalkan dan mengevaluasi tanggapan terhadap hasil audit, memastikan tingkat kepatuhan, serta menyusun laporan yang terintegrasi dengan bisnis.

Kebijakan ini dapat dituangkan dalam pendefinisian kebutuhan persyaratan compliance terhadap aturan tertentu (misal Sarbanes-Oxley, Basel II, PCI, Peraturan Bank Indonesia no.9/15/PB1/2007,dll), prosedur pengelolaan review terhadap audit eksternal, dan prosedur penyusunan laporan yang terintegrasi dengan laporan bisnis.

G. Ketentuan Operasional Teknologi Informasi

1. Kebijakan Operasional Teknologi Informasi

Kebijakan Operasional ini adalah untuk menerapkan kebijakan-kebijakan yang berkaitan dengan operasional dibidang Teknologi Informasi di PT Usaha Gedung Mandiri yang diatur sebagai berikut:

- a. Seluruh karyawan atau pengguna yang sudah mendapatkan ijin dari Manajer TI, bertanggung jawab dan wajib untuk mematuhi semua kebijakan yang tercantum dalam kebijakan ini ini.
- b. Seluruh infrastruktur IT di Perusahaan berada dibawah tanggung jawab Unit kerja TI. Tidak diijinkan untuk siapapun juga untuk meniru, merubah, menambah atau melampirkan sesuatu ke dalam infrastruktur IT tanpa persetujuan tertulis dari Unit Kerja TI. Contoh dari infrastruktur IT, namun tidak terbatas pada, adalah data *log is* dan fisik serta koneksi nirkabel, *server*, konferensi video, *email*, keamanan, otentifikasi dan operasional dari pusat data.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 28 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

- c. Kebijakan ini berlaku bagi setiap dan seluruh karyawan Perusahaan dan bagi setiap dan seluruh pengguna yang sudah mendapatkan ijin dari Unit Kerja TI.
- d. Adanya pelanggaran terhadap klausa-klausa yang terdapat dalam KO ini akan mengakibatkan penerapan tindak disipliner atau konsekuensi lainnya sesuai peraturan, SPO Tata Tertib dan Kedisiplinan Pegawai , Peraturan Perusahaan, atau bentuk lainnya yang mencantumkan konsekuensi terkait dengan pelanggaran Kebijakan ini.

2. Perilaku yang Bertanggung Jawab

Ijin penggunaan sumber daya IT dari Perusahaan dapat sewaktu-waktu dicabut untuk sementara atau permanen disebabkan oleh perilaku yang tidak bertanggung jawab. Perilaku yang tidak bertanggung jawab antara lain sebagai berikut:

- a. Menempatkan informasi yang tidak benar ke dalam sistem.
- b. Penggunaan bahasa yang kasar atau tidak senonoh dalam pesan yang bersifat baik, publik atau pribadi, juga segala sesuatu yang dapat mengakibatkan terhambat atau hilangnya data dalam sistem dan jaringan Perusahaan.

3. Penggunaan *Email* Perusahaan dan Data Lainnya

Harap diperhatikan bahwa segala bentuk komunikasi via *email*, messenger atau bentuk lainnya, yang menggunakan dan/atau disimpan dalam peralatan Perusahaan merupakan hak milik penuh dan eksklusif perusahaan. Pihak Perusahaan dan personel yang berwenang memiliki wewenang untuk mengakses materi *email* atau data atau dokumen dalam unit komputer karyawan setiap saat diperlukan oleh pihak Perusahaan.

Seluruh media komunikasi elektronik, penyimpanan data maupun akses yang dihasilkan atau disimpan di peralatan perusahaan, di tempat kerja atau merupakan materi pekerjaan dari perusahaan dianggap bukan sebagai milik pribadi karyawan, namun sebagai hak milik penuh dan eksklusif perusahaan.

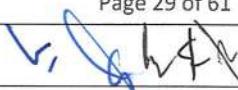
4. Materi yang Mengandung Konten Seksual

Karyawan dilarang keras untuk membuka, mengirim, menerima, mendistribusikan, mencetak atau menyimpan dokumen dalam bentuk apapun, elektronik atau hardcopy yang mengandung konten seksual, yang dapat memberikan penilaian yang tidak baik terhadap sumber daya IT Perusahaan.

5. Kebijakan Umum

Seluruh karyawan dan pengguna yang sudah mendapatkan izin dari MIT, wajib mematuhi semua sebagai berikut:

- a. Melaporkan atau menginformasikan segala kelemahan dari sistem IT Perusahaan kepada Unit Kerja TI.
- b. Melaporkan atau menginformasikan kepada Unit Kerja TI setiap adanya kemungkinan penyalahgunaan atau pelafnggaran sistem IT sesuai dengan Ketentuan Perusahaan.
- c. Pengaksesan informasi hanya untuk informasi yang telah dimiliki secara sah dan legal atau yang dapat diakses secara merata oleh publik atau yang sudah memiliki ijin untuk mengakses. Hanya diizinkan untuk memakai komputer yang telah disiapkan atau hanya untuk tujuan khusus dimana sudah dikeluarkan persetujuannya oleh Unit kerja TI.
- d. Karyawan atau pengguna yang sudah mendapatkan ijin dari Unit Kerja TI, wajib menjaga kerahasiaan dari *User ID*, *password* atau sistem yang sedang digunakan dari pihak yang

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi	Halaman :	Page 29 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02
Tgl Berlaku :	27 Januari 2023	Revisi : 

tidak berwenang. Berbagi informasi dengan pihak lain yang tidak berwenang, walaupun dengan sesama rekan kerja diperusahaan, akan dianggap bertanggung jawab atas seluruh aktifitas penggunaan *account* bersangkutan.

- e. Dilarang keras memindahkan atau *install* perangkat lunak yang telah disediakan Perusahaan untuk komputer tertentu, ke komputer lainnya tanpa seijin Unit Kerja RSC dan atau ITBS.
- f. Dilarang untuk menyalahgunakan, mengancam atau menjiplak sistem teknik atau pemrograman, jaringan atau sumber dari internet, menghancurkan integritas dari data informasi, informasi dengan akses tertentu dan/atau menjalankan suatu sistem tanpa ijin tertulis dari Unit kerja RSC dan atau ITBS.
- g. Dilarang keras untuk memasang/*install* piranti keras atau piranti lunak, pada peralatan Perusahaan, yang tidak berkaitan dengan Perusahaan.
- h. Dilarang keras untuk mengubah atau mengutak-atik piranti keras atau piranti lunak milik Perusahaan tanpa seijin Unit kerja RSC dan atau ITBS.
- i. Dilarang keras untuk mengubah, memasang atau memindahkan piranti lunak untuk keamanan, namun tidak terbatas pada *spyware*, *Firewall*, *internet browser* atau *email client software*.
- j. Dilarang keras untuk memasang atau menggunakan aplikasi hasil modifikasi atau buatan sendiri pada peralatan atau sistem IT Perusahaan.
- k. Wajib melaporkan kepada Unit kerja TI apabila mengetahui terjadinya gangguan atau kerusakan pada piranti keras atau piranti lunak atau pada sistem IT Perusahaan. tidak diperbolehkan sama sekali untuk mencoba memperbaiki gangguan atau kerusakan tanpa ijin tertulis dari Unit kerja TI.
- l. Dilarang keras menempatkan materi yang mengandung konten seksual dalam bentuk apapun dan tidak berhubungan dengan pekerjaan, ke dalam sistem IT Perusahaan.
- m. Dilarang keras untuk memanfaatkan sistem atau peralatan IT Perusahaan bagi kepentingan pribadi yang bersifat komersial ataupun non-komersial, seperti, namun tidak terbatas pada, menjual atau,membagi akses *User ID* atau password dari sistem IT atau peralatan IT Perusahaan.
- n. Dilarang keras untuk menggunakan *email* atau *messaging service* untuk mengganggu atau mengintimidasi orang lain, seperti, namun tidak terbatas pada, pesan-pesan sampah atau *spam* yang tidak diinginkan dan tidak berhubungan dengan pekerjaan.
- o. Dilarang keras membuka *email* atau pesan dari siapapun yang terlihat mencurigakan dari sisi keamanan. *Email* atau pesan seperti tersebut harap dihapus dari inbox secepatnya. Apabila dianggap perlu, harap konsultasikan terlebih dahulu dengan Unit kerja TI sebelum membukanya atau menghapusnya. Kerusakan terhadap fasilitas IT Perusahaan yang disebabkan oleh ketidakwaspadaan pihak karyawan atau pengguna yang sudah mendapatkan ijin dari MIT, akan mendapat tindakan disipliner sesuai dengan peraturan Perusahaan yang berlaku.
- p. Dilarang keras menyimpan *file-file* musik atau film, yang tidak berhubungan dengan pekerjaan, ke dalam sistem IT Perusahaan. *File-file* tersebut akan dihapus dari *server* sewaktu-waktu tanpa adanya pemberitahuan terlebih dahulu.

**Standar Prosedur Operasional
Pengelolaan Teknologi Informasi (TI)**

Bab V Fungsi Teknologi Informasi



- q. Penggunaan *file sharing* yang berkapasitas besar hanya diperbolehkan dalam jaringan internal Perusahaan dengan ijin tertulis MIT.
- r. Penggunaan peralatan IT pribadi, seperti, namun tidak terbatas pada, laptop, flashdisk, bluetooth, camera atau komputer dengan menggunakan sistem jaringan Perusahaan hanya dapat dilakukan dengan ijin tertulis dari MIT.
- s. Dilarang keras untuk mendownload *file* yang tidak berhubungan dengan pekerjaan.
- t. Dilarang keras mengirim atau menerima *email* atau *file* terlampir (*attachment*) apapun juga yang melebihi kapasitas.
- u. Dilarang keras menjalankan bisnis pribadi dengan menggunakan fasilitas IT Perusahaan. Pelanggaran atas hal ini dapat mengakibatkan Pemutusan Hubungan Kerja (PHK) secara otomatis dan tanpa pemenuhan. kewajiban atau pemberian ganti rugi dalam bentuk apapun dari pihak Perusahaan.

H. Ketentuan Wi-Fi

1. Pengertian

Wi-Fi adalah protokol jaringan nirkabel yang digunakan oleh perangkat komputer untuk terhubung ke internet tanpa menggunakan kabel. Istilah Wi-Fi sendiri digunakan untuk menyebutkan LAN (Local Area Network) jenis *wireless* (nirkabel) berdasarkan standar protokol jaringan 802.11 IEEE.

Istilah Wi-Fi seringkali disamakan dengan internet. sedangkan Wi-Fi adalah protokol perantara yang membawa koneksi internet dengan standar koneksi nirkabel. Sehingga, dengan Wi-Fi setiap orang dapat menangkap sinyal internet tanpa harus menggunakan jaringan kabel.

2. Cara Kerja Wi-Fi

- a. Syarat utama agar membuat Wi-Fi bekerja adalah dengan menyediakan perangkat yang dapat mengatur lalu lintas internet seperti *router*. Nantinya, *router* akan menerima jaringan internet dari jasa penyedia layanan internet di luar jaringan.
- b. *Router* akan mengirimkan jaringan tersebut ke perangkat terdekat yang dapat menerimanya. Seperti *handphone*, komputer, laptop, *smart TV* maupun perangkat lain yang dapat menerima koneksi internet melalui Wi-Fi dari *router* tersebut.
- c. Saat berada di tempat yang memiliki jaringan Wi-Fi, umumnya akan ada satu atau lebih *router* yang diletakkan di tempat tersebut. Selain router, perangkat seperti handphone maupun komputer juga dapat bekerja layaknya *router*, dengan mengaktifkan *hotspot* Wi-Fi untuk dapat berbagi koneksi internet nirkabel.

3. Perangkat Wi-Fi

Selain *router*, ada beberapa perangkat keras (*hardware*) lainnya yang dibutuhkan untuk membangun jaringan Wi-Fi seperti yang akan dijelaskan di bawah ini:

a. *Wireless Network Adapter*

Salah satu perangkat yang digunakan untuk membangun jaringan Wi-Fi adalah *wireless adapter* atau *Wi-Fi adapter*. Perangkat yang satu ini berfungsi sebagai alat yang dipakai pada perangkat komputer agar dapat tersambung dengan jaringan Wi-Fi yang ada di sekitarnya. *Wireless adapter* biasanya berbentuk USB atau slot PCI. Sedangkan pada laptop maupun handphone, umumnya sudah dilengkapi dengan *wireless adapter*.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi	Halaman :	Page 31 of 61
No Reg :	001/2023/SPO/RSC	Diverifikasi oleh :
Tgl Berlaku :	27 Januari 2023	Revisi :

b. *Wireless Router* atau *Wireless Access Point*

Wireless router adalah perangkat yang berfungsi sebagai pengatur lalu lintas jaringan yang dapat menerima dan mengirimkan sinyal internet melalui perantara Wi-Fi. *Wireless router* sering juga disebut sebagai *wireless access point*.

c. Antena *Wireless*

Antena *wireless* merupakan perangkat yang dapat mengirim dan menerima sinyal elektromagnetik. *Wireless router* memanfaatkan antena jenis ini untuk memperluas area jangkauan.

d. *Wireless Repeater*

Perangkat lain yang digunakan untuk membangun jaringan Wi-Fi adalah *wireless repeater*. Fungsinya untuk menguatkan sinyal yang mulai melemah ketika berada di jangkauan yang jauh dari pusat. *Wireless repeater* perlu dihubungkan pada *wireless router* agar dapat bekerja.

4. Keunggulan dan Kekurangan Wi-Fi

a. Keunggulan

1) **Kenyamanan**

Dengan sifatnya yang nirkabel, pengguna Wi-Fi bisa lebih nyaman mengakses internet dari semua lokasi yang terjangkau area Wi-Fi. Dengan begitu tidak perlu lagi berada di satu tempat saja untuk dapat menggunakan internet.

2) **Mobilitas**

Berkat adanya jaringan nirkabel, dapat mengakses internet dengan lebih fleksibel dari mana saja.

3) **Produktivitas**

Penggunaan Wi-Fi dapat meningkatkan produktivitas, terlebih jika membutuhkan jaringan internet untuk dapat bekerja. Wi-Fi memungkinkan untuk tetap terhubung dengan internet meskipun kamu berada di tempat yang berpindah-pindah.

4) **Perluasan**

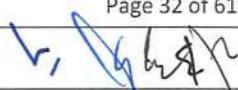
Jaringan Wi-Fi nirkabel hanya membutuhkan *router* maupun antena tambahan untuk memperluas jangkauannya. Berbeda dengan jaringan kabel yang memiliki struktur kabel kompleks untuk dapat memperluas jangkauan.

5) **Penggunaan**

Kelebihan lain Wi-Fi adalah penggunaannya yang mudah. Hanya perlu menghubungkan perangkat komputer dengan Wi-Fi untuk dapat menikmati akses internet. Sedangkan jaringan kabel memerlukan kabel tambahan jika ingin menambahkan pengguna.

6) **Biaya**

Biaya pemeliharaan yang dibutuhkan Wi-Fi nirkabel akan lebih sedikit jika dibandingkan dengan biaya perawatan jaringan kabel.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 32 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

b. Kekurangan Wi-Fi

1) Keamanan

Wi-Fi memiliki protokol jaringan keamanan seperti WPA2-PSK. Namun, dengan berkembangnya kejahatan *cyber* saat ini, kamu mungkin memerlukan sistem keamanan tambahan. Terlebih, jika menggunakan Wi-Fi untuk mengakses informasi atau aktivitas pribadi di internet.

2) Jangkauan

Protokol jaringan 802.11 IEEE pada Wi-Fi umumnya memiliki jangkauan yang tidak terlalu luas. Untuk memperluasnya, dibutuhkan perangkat tambahan seperti antena *wireless* dan tentunya hal ini memerlukan biaya tambahan.

3) Keandalan

Sama halnya dengan transmisi frekuensi radio lainnya, sinyal pada jaringan Wi-Fi terkadang mengalami berbagai macam gangguan. Termasuk, gangguan yang berada di luar kendali administrator jaringan.

4) Kecepatan

Kecepatan jaringan Wi-Fi adalah 1 hingga 54 Mbps, berbeda dengan jaringan kabel yang dapat mencapai 100 Mbps hingga beberapa Gbps. Hal ini membuat Wi-Fi lebih lambat jika dibandingkan dengan jaringan kabel.

I. Ketentuan Insiden Keamanan Informasi

A. Insiden Keamanan Informasi

Istilah insiden keamanan informasi memiliki beragam definisi. Kejadian insiden keamanan informasi dapat beragam, diantaranya adalah pencurian data, bencana alam, bahaya dari lingkungan sekitar seperti kebakaran, kegagalan saluran data, *System crash*, paket *flooding*, penggunaan akses atau penggunaan sumber daya sistem yang tidak sah, penggunaan akun pengguna lain secara tidak sah, penggunaan hak sistem tanpa izin, perusakan web, penetrasi/intrusi sistem, maupun serangan virus yang masif.

B. Manajemen Insiden Keamanan Informasi

Manajemen insiden keamanan informasi merupakan satu atau serangkaian proses mendeteksi dan merespon insiden keamanan informasi, termasuk di dalamnya adalah proses pembelajaran insiden dan menggunakan hasil pembelajaran yang didapat sebagai bagian dari input dalam keseluruhan proses manajemen selanjutnya. Manajemen insiden keamanan informasi dapat diadopsi dari berbagai macam *framework* atau standar yang ada di dunia.

Seluruh standar insiden manajemen keamanan informasi mempunyai kesamaan, yaitu terdiri dari beberapa fase/tahapan dalam proses manajemennya. Beberapa standar memiliki fase persiapan (*preparation*) yang digunakan untuk mempersiapkan kapasitas dalam penanganan insiden. Di fase berikutnya, hampir seluruh standar mempunyai fase deteksi, analisis dan respon atas insiden. Sedangkan fase pembelajaran (*lesson learned*) terdapat di semua standar.

Respon insiden (*incident response*) merupakan salah satu bagian dari proses penanganan insiden (*incident handling*), dan penanganan insiden merupakan bagian dari keseluruhan

**Standar Prosedur Operasional
Pengelolaan Teknologi Informasi (TI)**

Bab V Fungsi Teknologi Informasi



manajemen insiden (incident management). Penanganan insiden dilakukan oleh suatu tim respon insiden yang dapat dinamakan IRT (*Incident response Team*), CSIRT (*Computer Security Incident response Team*), atau CERT (*Computer Emergency Response Team*).

Beberapa tujuan utama manajemen insiden keamanan informasi adalah:

1. Menghindari terjadinya insiden kemanan informasi.
2. Meminimalkan dampak insiden keamanan informasi terhadap kerahasiaan, ketersediaan, atau integritas layanan, aset informasi, dan operasi organisasi.
3. Mengancaman dan kerentanan saat terjadi insiden.
4. Meningkatkan koordinasi dan manajemen insiden keamanan informasi dalam industry investasi.
5. Mengurangi dampak biaya yang disebabkan oleh insiden keamanan informasi.
6. Melaporkan temuan kepada manajemen eksekutif.

**Standar Prosedur Operasional
Pengelolaan Teknologi Informasi (TI)**

Bab VI Keamanan Fisik



Ranah persoalan (*domain*) keamanan fisik (*physical Security*) dalam keamanan sistem informasi amatlah adalah menguji elemen-elemen lingkungan fisik dan infrastruktur pendukung yang menjaga kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) sebuah sistem informasi. *Domain* keamanan fisik membahas ancaman, kerawanan, dan tindakan yang dapat diambil untuk memberi perlindungan fisik terhadap sumber daya organisasi dan informasi yang sensitif. Sumberdaya ini meliputi personel, fasilitas tempat mereka bekerja, data, peralatan, sistem pendukung, dan media yang digunakan.

Keamanan fisik sering mengacu pada tindakan yang diambil untuk melindungi sistem, gedung, dan infrastruktur pendukung yang terkait terhadap ancaman yang berhubungan dengan lingkungan fisik. Keamanan fisik komputer dapat juga didefinisikan sebagai proses yang digunakan untuk mengontrol personel, bangunan fisik, peralatan, dan data yang terlibat dalam pengolahan informasi.

A. Risiko Keamanan Fisik

Beberapa contoh risiko dalam keamanan fisik adalah seperti berikut ini:

1. Interupsi dalam menyediakan layanan computer - ketersediaan
2. Kerusakan fisik - ketersediaan
3. Keterungkapan informasi - kerahasiaan
4. Kehilangan kendali atas sistem - keutuhan
5. Pencurian-kerahasiaan, keutuhan, dan ketersediaan

B. Kontrol Keamanan Fisik

Kontrol keamanan fisik dibagi dalam 3 grup yaitu:

1. Kontrol administratif, adalah area perlindungan keamanan fisik yang dilakukan dengan langkah-langkah administratif. Langkah ini mencakup prosedur emergensi, kontrol personel (dalam area sumber daya manusia), perencanaan, dan penerapan kebijakan. Kontrol administratif yang terdiri dari:
 - a. Perencanaan kebutuhan fasilitas adalah konsep akan perlunya perencanaan kontrol keamanan fisik pada tahap awal dari pembangunan fasilitas data. Beberapa elemen keamanan fisik dalam tahap pembangunan meliputi memilih dan merencanakan lokasi site yang aman.
 - b. Manajemen keamanan fasilitas terdiri dari jejak audit dan prosedur emergensi. Keduanya adalah elemen kontrol keamanan administratif yang tidak berhubungan dengan perencanaan awal penentuan site yang aman, namun dibutuhkan sebagai dasar operasionalnya.
 - c. Kontrol personel administratif mencakup proses administratif yang biasa diimplementasikan oleh departemen SDM selama perekrutan dan pemecatan pegawai.
2. Kontrol lingkungan dan keamanan hidup, dianggap sebagai kontrol kemanan fisik yang dibutuhkan untuk menjamin baik lingkungan operasi komputer maupun lingkungan operasi personel.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi	Halaman :	Page 35 of 61
No Reg : 001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :
Tgl Berlaku : 27 Januari 2023	Revisi :	

**Standar Prosedur Operasional
Pengelolaan Teknologi Informasi (TI)**

Bab VI Keamanan Fisik



3. Kontrol fisik dan teknis

Area yang dicakup dalam Kontrol fisik dan teknis adalah kontrol lingkungan, perlindungan kebakaran, daya listrik, penjaga, dan kunci. Elemen-elemen *control* fisik dan teknis diantaranya adalah sebagai berikut:

a. CCTV (*Closed-Circuit Television*)

Fungsi utama CCTV meningkatkan keamanan. Itu juga berarti upaya pencegahan terhadap tindak kriminal dan kejahatan. CCTV merekam dan menampilkan video secara langsung memantau suatu tempat. Di kawasan yang gelap atau tanpa penerangan sedikit pun, CCTV tetap akan berfungsi maksimal menampilkan sorotannya. Manfaat dari CCTV.

Pengawasan visual atau perangkat perekam seperti CCTV digunakan sebagai tambahan penjaga untuk meningkatkan kemampuan pengawasan dan merekam peristiwa untuk analisis di masa depan atau untuk kepentingan bukti kejahatan dan penuntutan. Perangkat ini bisa berupa fotografik seperti kamera foto atau kamera video, atau elektronik seperti kamera CCTV. CCTV dapat digunakan untuk memonitor peristiwa langsung yang terjadi di daerah yang jauh dari jangkauan penjaga, atau dapat digunakan bersama VCR sebagai metode yang efektif dalam biaya untuk merekam peristiwa. Terdapat 2 Jenis CCTV yaitu:

1) CCTV Analog

Analog CCTV adalah versi kamera yang menggunakan sistem dan memiliki kualitas lama. Berbeda dengan jenis baru, varian ini masih beroperasi secara manual yaitu membutuhkan memori guna menyimpan video.

2) CCTV IP Camera

Variasi IP Camera CCTV adalah jenis baru dan lebih mutakhir dari kamera pengintai ini memiliki penyimpanan rekaman yang lebih fleksibel serta menggunakan koneksi internet. Sehubungan dengan kualitas kamera, tentu saja IP Camera CCTV adalah yang paling bagus dikarenakan hasil gambar atau rekaman yang diproduksi jauh lebih jernih karena memiliki resolusi tinggi.

b. Kartu Akses Keamanan (*Security Access Card*)

Kartu akses keamanan adalah metode umum dalam kontrol akses fisik. Ada dua tipe umum kartu akses keamanan yaitu :

1) Kartu Gambar Foto (*dumb card*)

Kartu jenis ini membutuhkan penjaga untuk membuat keputusan mengenai keabsahannya, dimana kartu ini menggunakan foto (*photo image card*) yaitu kartu identifikasi yang sederhana dengan adanya foto pemegang kartu sebagai alat identifikasinya. Ini adalah kartu ID standar yang berfoto, seperti kartu SIM ataupun kartu pegawai. Kartu ini disebut bodoh karena tidak mempunyai kecerdasan di dalamnya, dan perlu dibuat keputusan aktif oleh personel di pintu masuk sebagai otentikasi

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 36 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

**Standar Prosedur Operasional
Pengelolaan Teknologi Informasi (TI)**

Bab VI Keamanan Fisik



2) Kartu Bersandi Digital (*Smart Card*)

Kartu jenis ini membuat keputusan masuk secara elektronik (tidak membutuhkan penjaga untuk membuat keputusan masuk mengenai keabsahannya). Kartu sandi digital mengandung chip atau sandi garis magnetik (sebagai tambahan atas foto pemegang kartu). Pembaca kartu dapat diprogram untuk menerima akses berdasarkan komputer kontrol akses online yang juga menyediakan informasi mengenai tanggal dan waktu akses masuk. Kartu jenis ini juga bisa membuat pengelompokan akses banyak tingkat.

Bentuk umum dari kartu sandi digital, yaitu *smart card*. Kartu *smart card* memiliki kode garis magnetik atau chip IC (*Integrated Circuit*) kecil yang tertanam di dalamnya. Penggunaan kartu ini membutuhkan pengetahuan *password* atau PIN (*Personal Identification Number*) untuk mendapat akses masuk. Kartu ATM adalah contoh dari kartu model ini. Kartu ini mengandung prosesor tersandikan dengan protokol otentikasi sistem, ruang memori read-only untuk program dan data, dan beberapa diantaranya dilengkapi dengan sejenis antarmuka pengguna (*user interface*).

Dalam beberapa skenario, kartu *smart card* dapat dipasangkan dengan token otentikasi yang membangkitkan password atau PIN yang sekali pakai (*one-time*) atau berupa *challenge-response*. Sementara otentikasi *dual-factor* paling banyak digunakan untuk akses *log in* layanan jaringan, kartu *smart card* bisa dikombinasikan dengan *card reader* yang pintar untuk menyediakan kontrol yang sangat kuat terhadap akses fasilitas.

A. Proses Manajemen Perubahan

Perubahan bertujuan agar perusahaan tidak menjadi statis melainkan tetap dinamis dalam menghadapi perkembangan zaman, kemajuan teknologi dan dibidang pelayanan masyarakat adalah peningkatan kesadaran masyarakat akan pelayanan yang berkualitas.

Perubahan terdiri dari 3 tipe yang berbeda, dimana setiap tipe memerlukan strategi manajemen perubahan yang berbeda pula. Tiga macam perubahan tersebut adalah:

1. Perubahan Rutin, dimana telah direncanakan dan dibangun melalui proses organisasi.
2. Perubahan Peningkatan, yang mencakup keuntungan atau nilai yang telah dicapai organisasi.
3. Perubahan Inovatif, yang mencakup cara bagaimana organisasi memberikan pelayanannya.

Pemanfaatan atau implementasi teknologi informasi dalam kegiatan operasional organisasi akan memberikan dampak yang cukup signifikan bukan hanya dari efisiensi kerja tetapi juga terhadap budaya kerja baik secara personal, antar unit, maupun keseluruhan institusi. Pengelolaan administrasi kerja berbasis teknologi informasi juga harus mempertimbangkan pengembangan sumber daya manusia (SDM) untuk mendukung optimalisasi pada pemanfaatan atau implementasi teknologi informasi yang bertahap yang dimulai dengan perencanaan, pengembangan, ahli kelola, operasional sampai dengan tahap pemeliharaan.

Dengan adanya teknologi informasi, maka produktivitas suatu organisasi atau perusahaan akan meningkat, serta dapat membuat model bisnis yang sulit ditiru oleh pesaing, karena pada dasarnya peranan teknologi informasi bagi setiap perusahaan bersifat unik dan spesifik. Hal tersebut disebabkan karena masing-masing organisasi atau perusahaan memiliki strategi yang berbeda satu dengan yang lainnya.

Pemanfaatan teknologi informasi dalam suatu organisasi atau perusahaan juga berkaitan dengan keunggulan kompetitif untuk meningkatkan kualitas informasi, pengawasan kinerja organisasi atau perusahaan menggunakan teknologi informasi baik sebagai alat bantu maupun strategi yang tangguh untuk mengintegrasikan dan mengolah data dengan cepat dan akurat serta untuk penciptaan produk layanan baru sebagai daya saing untuk menghadapi kompetisi.

Selain itu implementasi atau pemanfaatan teknologi informasi memiliki dampak positif yang secara umum adalah terjadi efisiensi waktu dan biaya yang secara jangka panjang akan memberikan keuntungan ekonomis yang sangat tinggi. Oleh karena itu, pengoperasian secara optimal juga harus diperhatikan, agar semua perangkat teknologi informasi bersifat multi fungsi sehingga dalam pengembangan selanjutnya diupayakan terjadi integrasi perangkat.

Pemanfaatan teknologi informasi akan melibatkan semua karyawan dalam organisasi yang dioperasikan secara rutin oleh staf administrasi dan bagian teknologi informasi. Karyawan dengan kualifikasi tertentu baik bagian teknologi informasi maupun bagian lain perlu dilibatkan selain untuk memberikan masukan juga untuk mempersiapkan karyawan dalam menghadapi perubahan. Di sisi lain, diperlukan kesadaran personal lainnya tehadap manfaat sistem bagi dirinya dan kemudahan penggunaannya secara bertahap akan memberikan motivasi untuk meningkatkan kemampuan mereka.

B. Implementasi Teknologi

Pemanfaatan atau implementasi teknologi dalam kegiatan operasional organisasi akan memberikan dampak yang cukup signifikan bukan hanya dari efisiensi kerja, namun juga terhadap budaya kerja baik secara personal, antarunit, maupun keseluruhan intuisi. Berdasarkan struktur organisasi, pemanfaatan teknologi informasi di klasifikasikan menjadi tiga kategori, yaitu:

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 38 of 61
No Reg :	001/2023/SPO/RSC	Edisi :02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

1. Perbaikan Efisiensi, Pemanfaatan teknologi informasi untuk perbaikan efisiensi diterapkan pada level operasional organisasi. Pada kategori ini, pemanfaatan teknologi informasi diukur dengan penurunan waktu dan biaya proses.
2. Perbaikan Efektivitas, Pemanfaatan teknologi informasi untuk perbaikan efektivitas diterapkan pada level manajerial organisasi. Pada kategori ini pemanfaatan teknologi informasi ini diukur dengan kemudahan dan kecepatan memperoleh status pencapaian target organisasi.
3. Pemanfaatan teknologi informasi untuk strategic *improvement* (perbaikan daya saing) diterapkan pada level eksekutif organisasi. Pada kategori ini, pemanfaatan teknologi informasi diukur dengan kemudahan dan ketepatan pengambilan keputusan oleh eksekutif.

C. Peran Teknologi Informasi

Penggunaan TI (teknologi informasi) dalam sebuah organisasi sangatlah penting, dan untuk menerapkan TI tersebut haruslah dilihat karakteristik organisasi tersebut sebelumnya. Terdapat lima peranan mendasar teknologi informasi di sebuah perusahaan atau organisasi, yaitu:

1. Fungsi Operasional. Membuat struktur organisasi menjadi lebih ramping telah diambil alih fungsinya oleh teknologi informasi lantaran sifat penggunaannya yang menyebar di seluruh fungsi organisasi, unit terkait dengan manajemen teknologi informasi akan menjalankan fungsinya sebagai *supporting agency* dimana teknologi informasi dianggap sebagai *firm infrastructure*.
2. Fungsi *Monitoring and Control*. Mengandung arti bahwa keberadaan teknologi informasi akan menjadi bagian yang tidak terpisahkan dengan aktivitas di level manajerial embedded di dalam setiap fungsi manajer. Sehingga struktur organisasi unit terkait dengannya harus dapat memiliki span of *control* atau *peer relationship* yang memungkinkan terjadinya interaksi efektif dengan para manajer di perusahaan terkait.
3. Fungsi *Planning and Decision*. Keberadaan teknologi informasi dianggap sebagai enabler dari rencana rencana organisasi dan merupakan sebuah knowledge generator bagi para pimpinan perusahaan yang dihadapkan pada realitas untuk mengambil sejumlah keputusan penting sehari-harinya. Tidak jarang organisasi yang pada akhirnya memilih menempatkan unit teknologi informasi sebagai bagian dari fungsi perencanaan dan/atau pengembangan korporat karena fungsi strategis tersebut.
4. Fungsi *Communication*. Secara prinsip termasuk ke dalam *firm infrastructure* dalam era organisasi modern, dimana teknologi informasi ditempatkan posisinya sebagai sarana atau media individu perusahaan dalam berkomunikasi, berkolaborasi, berkooperasi, dan berinteraksi.
5. Fungsi Interorganisational. Merupakan sebuah peranan yang cukup unik karena dipicu oleh semangat globalisasi yang memaksa perusahaan untuk melakukan kolaborasi atau menjalin kemitraan dengan sejumlah perusahaan lain.

**Standar Prosedur Operasional
Pengelolaan Teknologi Informasi (TI)**

Bab VIII Multi Factor Authentication (MFA)



Autentikasi multi-faktor (MFA) adalah komponen manajemen akses yang mengharuskan pengguna untuk membuktikan identitas mereka menggunakan setidaknya dua faktor verifikasi yang berbeda sebelum mendapatkan akses ke situs web, aplikasi seluler, atau sumber daya online lainnya. Dengan MFA, jika satu faktor dikompromikan, penyerang masih memiliki setidaknya satu penghalang lagi untuk ditembus sebelum mereka bisa mendapatkan akses ke akun target.

A. Metode Autentifikasi

Jika hanya menggunakan kata sandi untuk mengautentikasi pengguna, kata sandi tersebut meninggalkan vektor yang tidak aman untuk diserang. Jika kata sandi lemah atau telah diekspos di tempat lain, penyerang dapat menggunakananya untuk mendapatkan akses. Jika mewajibkan bentuk autentikasi kedua, keamanan ditingkatkan karena faktor tambahan ini bukan sesuatu yang mudah didapatkan atau diduplikasi oleh penyerang. Autentikasi MultiFaktor bekerja dengan meminta dua atau lebih metode autentifikasi berikut ini:

1. Sesuatu yang diketahui, biasanya kata sandi.
2. Sesuatu yang dimiliki, seperti perangkat tepercaya yang tidak mudah diduplikasi, seperti ponsel atau kunci perangkat keras.
3. Sesuatu yang ada pada diri seperti biometrik pada sidik jari atau pemindaian wajah.

Multi-Factor Authentication juga dapat lebih mengamankan reset kata sandi. Ketika pengguna mendaftarkan diri untuk Autentikasi Multi-Faktor, mereka juga dapat mendaftar untuk reset kata sandi layanan mandiri dalam satu langkah. Administrator dapat memilih bentuk otentifikasi sekunder dan mengkonfigurasi tantangan untuk MFA berdasarkan keputusan konfigurasi.

Aplikasi atau layanan tidak perlu mengubah apa pun untuk menggunakan Autentikasi Multifaktor. Perintah verifikasi adalah bagian dari akses masuk, yang secara otomatis meminta dan memproses tantangan MFA jika diperlukan.

B. Metode Verifikasi yang tersedia

Saat pengguna masuk ke aplikasi atau layanan dan menerima perintah MFA, mereka dapat memilih salah satu formulir verifikasi tambahan yang terdaftar. Pengguna dapat mengakses *profile* untuk mengedit atau menambahkan metode verifikasi.

Formulir verifikasi tambahan berikut ini dapat digunakan dengan Multi-Factor Authentication:

1. Aplikasi Microsoft Authenticator
2. Windows Hello untuk Bisnis
3. Kunci keamanan FIDO2
4. Token perangkat keras
5. Token perangkat lunak
6. SMS
7. Panggilan suara

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 40 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

C. Manfaat Multi Factor Authentication

Sebagai bagian dari strategi keamanan, Perusahaan menggunakan MFA untuk mencapai:

1. Peningkatan keamanan

Autentikasi multi-faktor memberikan peningkatan keamanan dibandingkan kata sandi statis dan proses autentikasi faktor tunggal.

2. Kepatuhan terhadap peraturan

Otentikasi multi-faktor dapat membantu perusahaan mematuhi peraturan. Misalnya, MFA diperlukan untuk memenuhi persyaratan otentikasi yang kuat untuk *Strong Customer Authentication (SCA)*.

3. Pengalaman pengguna yang lebih baik

Memutus ketergantungan pada kata sandi dapat meningkatkan pengalaman pelanggan. Dengan berfokus pada tantangan otentikasi gesekan rendah, organisasi dapat meningkatkan keamanan dan meningkatkan pengalaman pengguna.

A. Pengertian *Host Hardening*

Pengertian *Host Hardening* adalah prosedur yang meminimalkan ancaman yang datang dengan mengatur konfigurasi dan menonaktifkan aplikasi dan layanan yang tidak diperlukan. Instalasi *Firewall*, instalasi antivirus, menghapus *cookie*, membuat *password*, menghapus program yang tidak diperlukan itu semua termasuk dalam *Host Hardening*.

Tujuan dari *Host Hardening* adalah untuk menghilangkan risiko ancaman yang bisa terjadi pada komputer. hal ini biasanya dilakukan dengan menghapus semua program/ file yang tidak diperlukan.

B. Macam-Macam & Implementasi Hardening System

1. Hardening System: *Security Policy*

Keberadaan dokumen "Kebijakan Keamanan" atau "Security Policies" merupakan sebuah infrastruktur keamanan yang harus dimiliki oleh sebuah organisasi atau perusahaan yang ingin melindungi aset informasi terpentingnya. Dokumen ini secara prinsip berisi berbagai cara (baca: kendali) yang perlu dilakukan untuk mengontrol manajemen, mekanisme, prosedur, dan tata cara dalam mengamankan informasi, baik secara langsung maupun tidak langsung. Karena berada pada tataran kebijakan, maka dokumen ini biasanya berisi hal-hal yang bersifat prinsip dan strategis.

Tujuan dasar dari *Security Policy* adalah sebagai berikut:

- a. Melindungi pengguna (*user*) dan informasi.
- b. Membuat aturan sebagai arahan untuk pengguna (*user*), sistem administrator, manajemen dan petugas keamanan sistem informasi (*IT Security*).
- c. Menetapkan petugas keamanan untuk pengawasan, penyelidikan atau pemeriksaan.
- d. Membantu mengurangi risiko yang mungkin akan muncul.
- e. Membantu arahan kepatuhan pada peraturan dan undang-undang.
- f. Menetapkan peraturan resmi perusahaan mengenai keamanan.

Pihak-pihak yang wajib menggunakan *IT Security Policy*:

- a. Manajemen – pada semua tingkatan.
- b. Technical staff – sistem administrator dan lainnya.
- c. Pengguna (*user*).

2. Hardening System: Kriptografi

Cryptographic protocol adalah suatu protokol yang menggunakan kriptografi. Protokol ini melibatkan sejumlah algoritma kriptografi, namun secara umum tujuan protokol lebih dari sekedar kerahasiaan. Pihak-pihak yang berpartisipasi mungkin saja ingin membagi sebagian rahasianya untuk menghitung sebuah nilai, menghasilkan urutan random, atau pun menandatangani kontrak secara bersamaan. Penggunaan kriptografi dalam sebuah protokol terutama ditujukan untuk mencegah ataupun mendeteksi adanya ditujukan untuk mencegah atau pun mendeteksi adanya *eavesdropping* dan *cheating*.

3. Hardening System: Firewall

Firewall adalah sebuah sistem yang didesain untuk mencegah akses yang tidak sah ke atau dari jaringan pribadi.

Firewall dapat diimplementasikan dalam perangkat keras dan perangkat lunak, atau kombinasi keduanya. *Firewall* sering digunakan untuk mencegah pengguna internet yang terhubung ke jaringan internet. Semua pesan yang masuk dan keluar dari internet harus melewati *Firewall*. *Firewall* ini bertindak sebagai pengawas setiap pesan dan memblok jika tidak memenuhi kriteria keamanan tertentu.

Fungsi *Firewall* sebagai pengontrol, mengawasi arus paket data yang mengalir di jaringan. Fungsi *Firewall* mengatur, memfilter dan mengontrol lalu lintas data yang diijinkan untuk mengakses jaringan privat yang dilindungi. Beberapa kriteria yang dilakukan *Firewall* apakah memperbolehkan paket data lewati atau tidak, antara lain:

- a. Alamat IP dari komputer sumber.
- b. Port TCP/UDP sumber dari sumber.
- c. Alamat IP dari komputer tujuan.
- d. Port TCP/UDP tujuan data pada komputer tujuan.
- e. Informasi dari header yang disimpan dalam paket data.

4. Hardening System: IDS (Intrusion Detection System)

Intrusion Detection Systems (IDS) adalah suatu tindakan untuk mendeteksi adanya trafik paket yang tidak diinginkan dalam sebuah jaringan atau device. Sebuah IDS dapat diimplementasikan melalui *software* atau aplikasi yang terinstall dalam sebuah device, dan aplikasi tersebut dapat memantau paket jaringan untuk mendeteksi adanya paket-paket ilegal seperti paket yang merusakkebijakan rules keamanan, dan paket yang ditujukan untuk mengambil hak akses suatu pengguna.

5. Hardening System: Backup

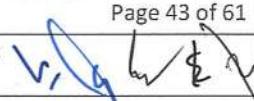
Backup yaitu membuat salinan data atau *file-file* komputer ke media penyimpanan lain untuk menjamin keamanan atau keselamatan data jika terjadi kerusakan data utama. *Backup* data dianjurkan secara berkala setiap periode tertentu. Dari beberapa kondisi digunakan sebuah *backup* yang beriringan dengan master datanya. Sebagai contoh pada sebuah jaringan komputer dibuat *server backup* yang berjalan beriringan dengan *server* utamanya. Jika *server* utama dan *server backup* diupdate secara bersamaan, maka jika *server* utama mati akan digantikan oleh *server backup*.

Kegiatan *backup* dalam *hardening System* memiliki beberapa tujuan, yaitu:

- a. Untuk menjaga keamanan data, terutama data yang memiliki kepentingan khusus.
- b. Untuk pengarsipan data.

6. Hardening System: Auditing System

Audit adalah suatu proses yang sistematik untuk mendapatkan dan mengevaluasi bukti secara obyektif mengenai pernyataan-pernyataan mengenai kegiatan dan kejadian dengan tujuan untuk menentukan tingkat kesuaian antara pernyataan-pernyataan tersebut dengan kriteria yang telah ditetapkan serta menyampaikan hasil-hasilnya kepada pihak yang berkepentingan.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 43 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

Ada beberapa manfaat untuk melakukan audit sistem jaringan, yaitu :

- a. Dapat mengidentifikasi kelebihan dan kekurangan suatu jaringan komputer.
- b. Dapat mengevaluasi sistem keamanan pada jaringan komputer.
- c. Memahami konsep dasar audit jaringan komputer.
- d. Memahami dasar-dasar teknik audit jaringan komputer.
- e. Mengetahui dan memahami fasilitas yang sudah ada, dan untuk lebih di tingkatkan.

Prosedur melakukan audit sistem:

- a. Memeriksa apakah ada fungsi manajemen Jaringan yang kuat dengan otoritas untuk membuat standar dan prosedur
- b. Memeriksa apakah tersedia dokumen mengenai inventarisasi peralatan Jaringan, termasuk dokumen penggantian peralatan
- c. Memeriksa apakah tersedia prosedur untuk memantau *network usage* untuk keperluan peningkatan kinerja dan penyelesaian masalah yang timbul
- d. Memeriksa apakah ada *control* secara aktif mengenai pelaksanaan standar untuk aplikasi-aplikasi on-line yang baru diimplementasikan.

7. Hardening System: Digital Forensik dan Penanganan Pasca Insiden.

Digital forensik adalah ilmu yang menganalisa barang bukti digital sehingga dapat dipertanggungjawabkan di pengadilan. Barang bukti digital merupakan hasil ekstrak dari barang bukti elektronik seperti Personal Komputer, mobilephone, notebook, server, alat teknologi apapun yang mempunyai media penyimpanan dan bisa dianalisa.

Digital forensik berkaitan dengan :

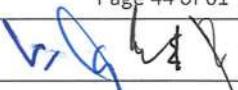
- a. Pengecekan koneksi aktif
- b. Pengecekan listening port pasca insiden
- c. Pengecekan proses yang aktif pasca insiden
- d. Pengecekan *log user* yang *log in*
- e. Pengecekan *log sistem*
- f. Pengecekan *log pengakses service*

C. Security Hardening

Security Hardening adalah suatu proses pengamanan sistem TI yang bertujuan untuk mengurangi kerentanan dan meningkatkan keamanan sistem TI terhadap berbagai serangan yang dapat terjadi. security hardening dapat membuat standar konfigurasi keamanan pada setiap server. Dalam proses security hardening terdapat banyak komponen yang wajib dikonfigurasi/atur, antara lain informasi server, pengaturan akses dan user, pengaturan password dan partisi, keamanan jaringan dan kernel, dan masih banyak lagi.

1. Langkah-langkah dalam melakukan security hardening

- a. Membuat dokumen standar security hardening untuk dijadikan acuan dan standar (benchmark), seperti dokumen dari Center for Internet Security (CIS).

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 44 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

- b. Membuat script agar implementasi security hardening dapat dipermudah.
- c. melakukan gap assessment untuk mengecek kondisi sistem dan membandingkannya dengan standar yang ada.
- d. Mengimplementasikan security hardening sesuai dengan standar yang telah ditentukan.
- e. Mendokumentasikan hasil dan keefektifitasan security hardening supaya bisa dijadikan tolak ukur di kemudian hari.

2. Tahapan proses yang memudahkan proses security hardening

- a. Melakukan Security Hardening saat instalasi baru, dimana semua konfigurasi operating system (OS) masih default dan belum ada aplikasi. Dengan demikian tidak ada dampak security haerdening terhadap jalannya aplikasi yang dapat mendisrupsi bisnis
- b. Melakukan backup setiap file serta konfigurasi yang diubah saat security hardening. Hal ini untuk mencegah terjadinya hal-hal yang tidak diinginkan saat kesalahan konfigurasi terjadi. Apabila file pam.d tidak di-backup, misalnya dan terjadi miskonfigurasi pada file tersebut, maka tidak akan bisa login dan wajib masuk emergency mode yang akan membutuhkan restart.
- c. Mempersiapkan koneksi cadangan (backup connection) agar dapat tetap mengakses server walaupun salah satu koneksi bermasalah. Sebagai contoh, apabila ingin mengkonfigurasi secure shell (SSH), siapkanlah koneksi lain, seperti akses desktop jarak jauh (remote desktop) ataupun console sehingga tetap bisa mengakses server kalau satu koneksi terputus akibat miskonfigurasi SSH.
- d. Melakukan pengecekan hasil konfigurasi untuk memastikan konfigurasi sudah diterapkan. Dengan pengaturan password, misalnya dapat mengecek apakah pengaturan sudah diterapkan dengan mencoba mengganti password user .
- e. Sesuaikan poin security hardening dengan kondisi server. Hal ini berarti jika memiliki server on premise maka putuskanlah koneksi SSH dengan Internet, tetapi jika menggunakan cloud service provider, koneksi SSH dengan Internet tidak boleh putus/disabled karena tidak memiliki akses lain untuk melakukan security hardening.
- f. Membuat template virtual machine (VM) yang sudah di-harden berupa file dengan format .ova. Jika security hardening dilakukan dalam jumlah besar, gunakanlah Ansible (Linux) atau Group Policy Object (Windows) untuk melakukan push policy ke setiap user yang menggunakan domain yang sama. Hal ini akan mempercepat proses security hardening.
- g. Jangka waktu untuk melakukan review hardening adalah 3 bulan sekali.

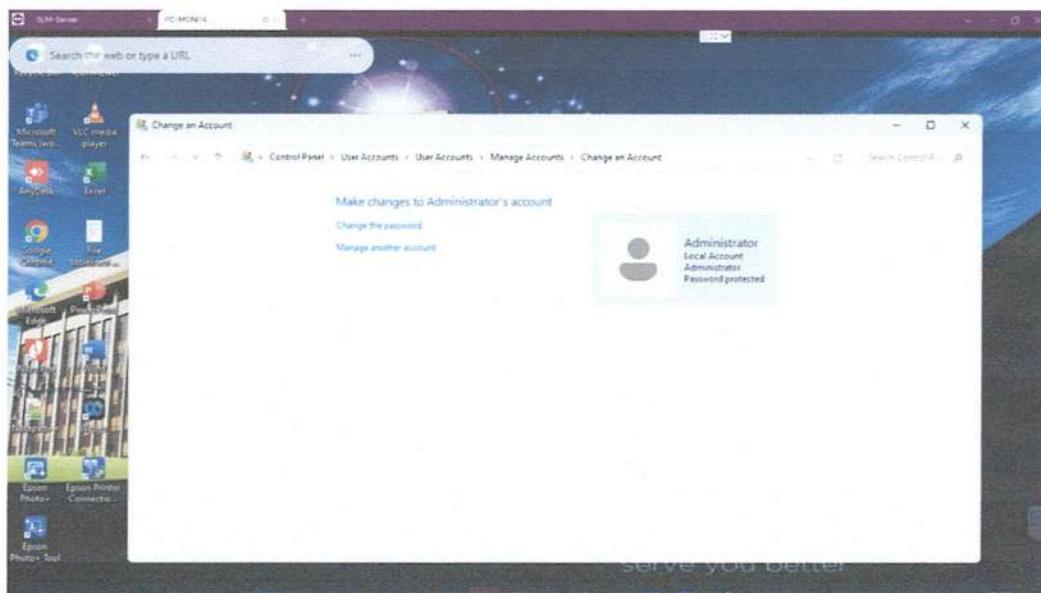
D. System Configuration Hardening

1. Membuat Checklist Hardening

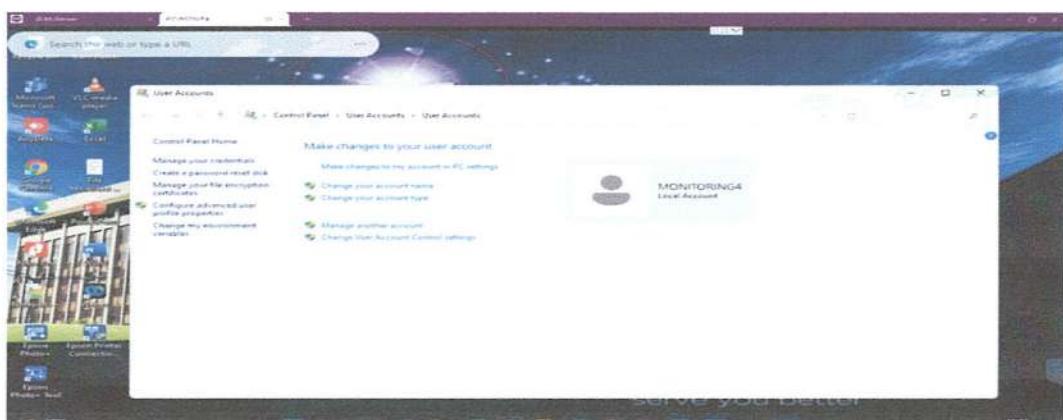
- Create Administrator Account & Password
- Create User
- Create Legal Notice
- Turn on Firewall
- Set Company Wallpaper
- Setup General Policy for Spesific Setting

2. Implementasi Hardening

Create Administrator Account & Password



Create User



Standar Prosedur Operasional Pengelolaan Teknologi Informasi (TI)

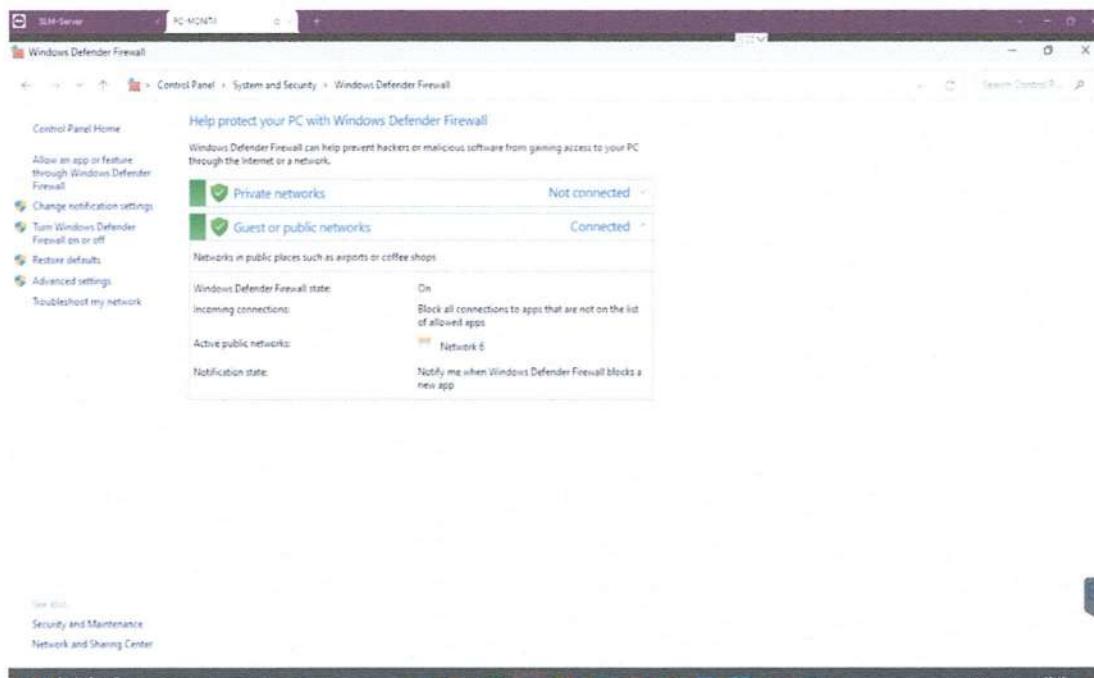
Bab IX Hardening System

UGmandiri
serve you better

○ Create Legal Notice



○ Turn on Firewall



**Standar Prosedur Operasional
Pengelolaan Teknologi Informasi (TI)**

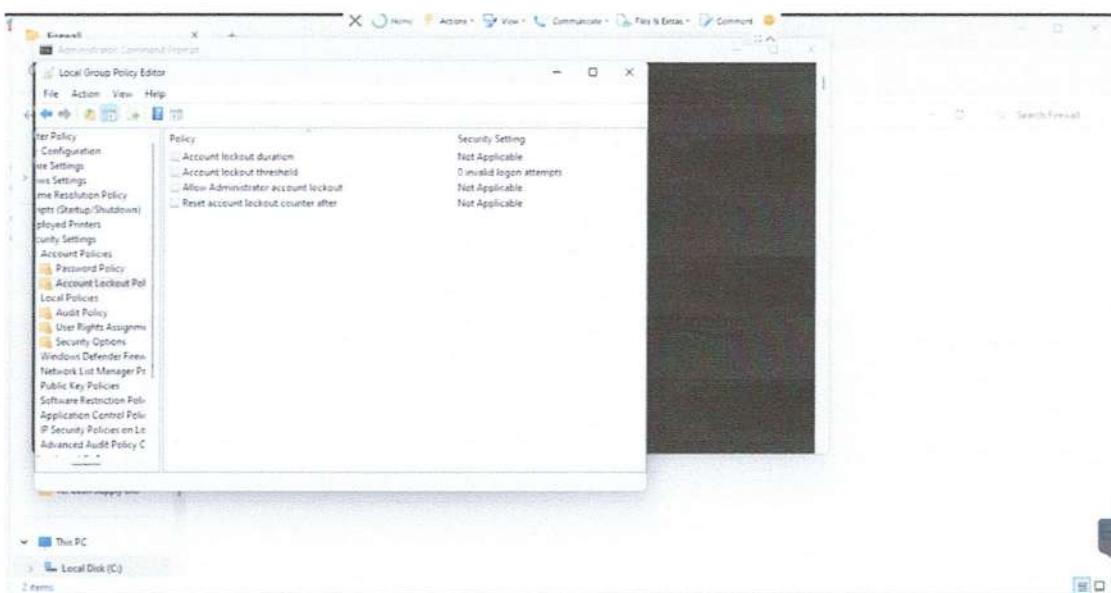
Bab IX Hardening System

UGmandiri
serve you better

○ Set Company Wallpaper



○ Setup General Policy for Spesific Setting

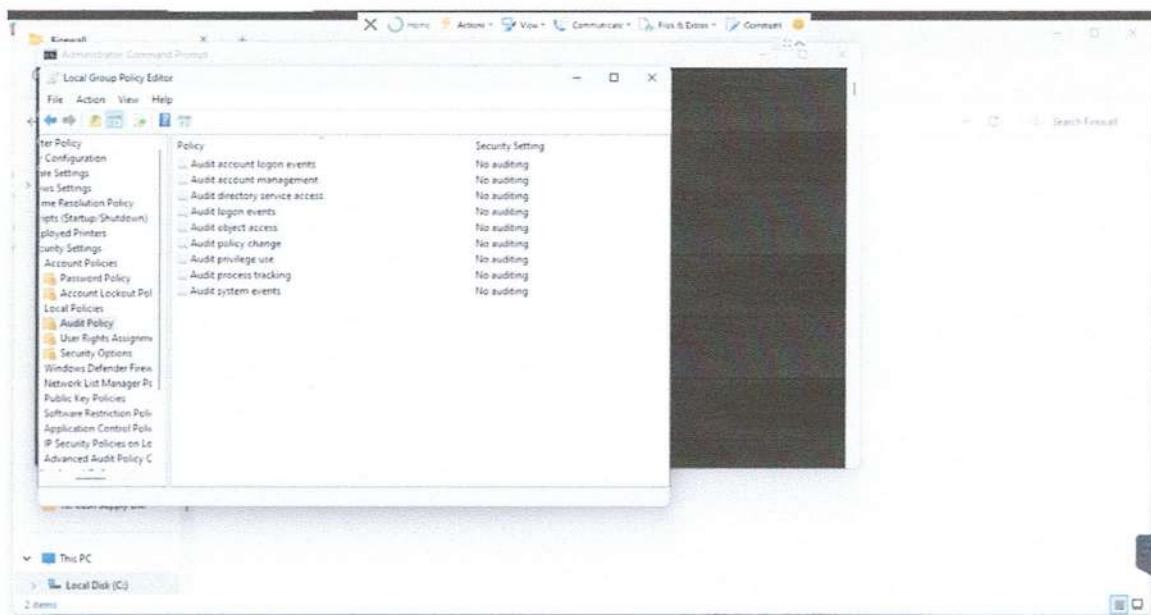
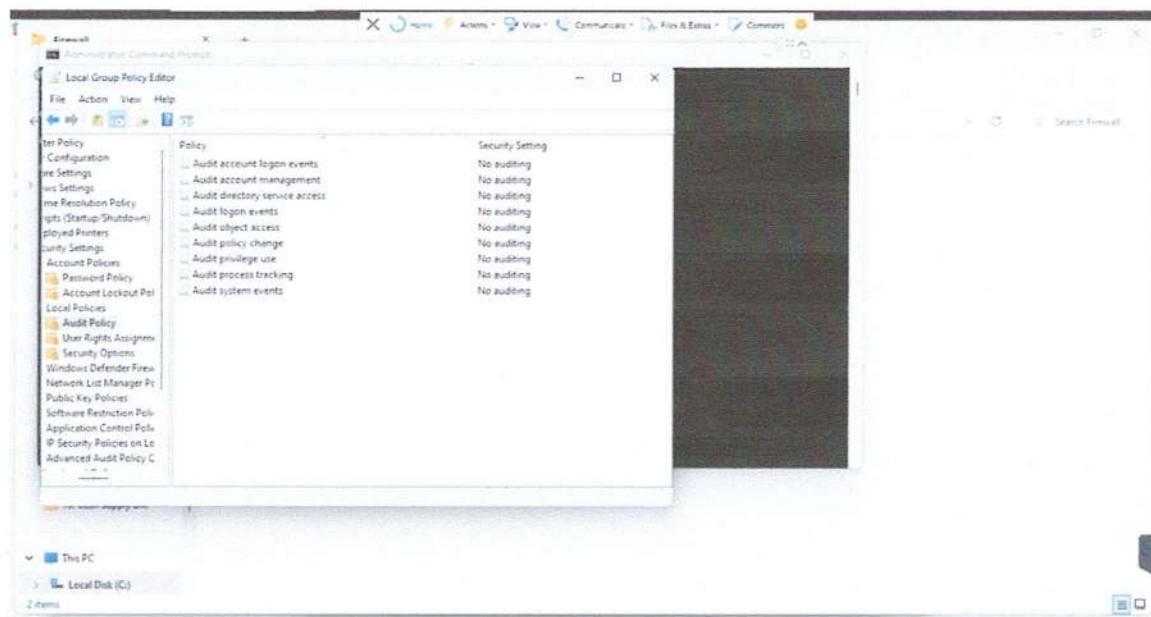


[Signature]

Standar Prosedur Operasional Pengelolaan Teknologi Informasi (TI)

Bab IX Hardening System

UGmandiri
serve you better



**Standar Prosedur Operasional
Pengelolaan Teknologi Informasi (TI)**

Bab X Keamanan Data



A. Ketentuan Antivirus

Virus adalah *file* yang mengganggu *System* operasional pada PC dan laptop, apabila laptop terkena virus maka secara otomatis kinerja laptop tidak akan maksimal, biasanya bentuk gangguan virus ini seperti kemampuan loading menjadi lebih lambat/ lemot, hilangnya *file-file* yang kita simpan secara tiba-tiba, laptop restart berulangkali, jika sudah berhadapan dengan virus yang hebat kadang OS akan terhapus, hal ini akan memaksa kita untuk melakukan instal ulang OS pada laptop.

Virus dalam komputer yaitu *file* pengganggu, setiap *file* yang dapat mengganggu kinerja OS adalah virus, *file* pengganggu ini bisa dalam bentuk *file* biasa yang sengaja kita simpan tetapi rusak, Worm, Kuda troya, Spyware, dan malware berbahaya yang terinstal baik secara sengaja maupun tidak. Sebenarnya kita tidak perlu takut terlalu berlebihan dengan apa yang di sebut virus dalam PC/laptop, selama kita mau melakukan langkah-langkah antisipasi dengan benar, maka kemungkinan virus dapat mengganggu laptop kita sangat kecil.

1. Antivirus

Antivirus adalah sebuah jenis perangkat lunak yang digunakan untuk mengamankan, mendeteksi, dan menghapus virus komputer dari sistem komputer. Antivirus disebut juga Virus Protection Software. Aplikasi ini dapat menentukan apakah sebuah sistem komputer telah terinfeksi dengan sebuah virus atau tidak. Umumnya, perangkat lunak ini berjalan di latar belakang (background) dan melakukan pemindaian terhadap semua berkas yang diakses (dibuka, dimodifikasi, atau ketika disimpan). Antivirus – antivirus terbaru sekarang tidak hanya mendeteksi virus. Program antivirus sekarang juga telah dilengkapi dengan kemampuan untuk mendeteksi spyware, rootkits, dan malware – malware lainnya. Tidak hanya itu, antivirus sekarang dilengkapi *firewall* untuk melindungi komputer dari serangan hacker dan anti *spam* untuk mencegah masuknya *spam* dan/atau virus ke inbox pengguna.

Antivirus berdasarkan penggunanya dibagi menjadi dua, yaitu Home User dan Network / Corporate User. Untuk home user, antivirus berjalan seperti biasa. Untuk versi jaringan (network), antivirus dapat melakukan scan di komputer – komputer client dan network drive. Selain itu, proses update komputer client dalam jaringan tidak harus langsung dari Internet. Komputer client dapat melakukan update langsung dari server jaringan.

2. Pencegahan Virus

Cara mencegah dan menghindari virus masuk pada komputer atau laptop:

- a. Gunakan antivirus yang kompatibel dan bonafit, selalu update antivirus tersebut.
- b. Jika komputer atau laptop sering digunakan browsing internet maka gunakan antivirus yang memiliki fitur Internet Security
- c. Aktifkan Firewall pada Windows yang anda gunakan.
- d. Selalu perbarui Security Update pada Windows Security.
- e. Jangan dibiasakan menyimpan data pada drive C terlalu lama.
- f. Kenali semua data yang anda simpan pada laptop, dan segera buang/hapus apabila ada data yang tidak anda kenal.
- g. Hapus *file* registry yang sudah tidak di perlukan secara teratur.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 50 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

**Standar Prosedur Operasional
Pengelolaan Teknologi Informasi (TI)**

Bab X Keamanan Data



- h. Apa bila akan memindahkan data dari device/perangkat lain, usahakan tidak membukanya dulu ketika masih terkoneksi, jadi langsung di send / copy kemudian lepaskan device / perangkat.
- i. Gunakan alat pembersihan seperti Ccleaner, TuneUp Utility, dsb.

B. Ketentuan *Removable* Media

Secara khusus, removable media merupakan perangkat penyimpanan data yang mampu melepaskan sistem komputer tanpa mematikan sistem. Contoh removable media antara lain *memory stick*, *pen drive*, *hard drive/ hard disk eksternal*, dan CD/DVD. Kebijakan penggunaan *removable* media bagi perusahaan adalah sebagai berikut:

1. Batasi penggunaan semua *removeable media* (perangkat media yang dapat dilepas) kecuali jika diizinkan secara khusus.
2. Terapkan perlindungan kata sandi atau *password*, terutama untuk melindungi informasi sensitif dan membatasi akses, semua media yang dapat dilepas harus dilindungi dengan kata sandi yang kuat.
3. Enkripsi informasi yang disimpan di *removeable media*, *disk* dan *device*. Jika penggunaan media yang dapat dilepas diperlukan, informasi di semua perangkat harus dienkripsi. Untuk tingkat enkripsinya sendiri, itu akan bergantung pada sensitivitas informasi yang disimpan di perangkat.
4. Jangan pernah menyalin *file* ke media eksternal kecuali jika diperlukan atau telah diberi wewenang.
5. Pindai semua media untuk mencari *malware*. Media yang dapat dilepas harus dipindai secara menyeluruh untuk mencari *malware* sebelum dibawa untuk digunakan atau diterima dari organisasi lain.
6. Jangan pernah meninggalkan media yang dapat dilepas tergeletak di sekitar lingkungan kerja. Kunci dengan aman saat tidak digunakan.
7. Nonaktifkan Bluetooth, Wi-Fi, dan layanan lainnya saat Anda tidak menggunakananya.
8. Jangan pernah mencoba mengakses *file* dari media yang dapat dilepas yang mungkin Anda temukan. Ini mungkin berisi virus yang akan menginfeksi sistem komputer dengan *malware*.
9. Saat menggunakan Bluetooth, setel ke mode “*undiscovered* atau tidak dapat ditemukan” untuk menyembunyikan perangkat dari perangkat yang tidak diautentikasi.
10. Segera laporkan perangkat yang hilang, sehingga semua *data collection* dapat ditindaklanjuti.
11. Gunakan *Security software* (perangkat lunak keamanan) dan atau selalu *update* atau perbarui semua perangkat lunaknya.

C. Ketentuan *Backup* Data

Backup adalah kegiatan penyalinan data yang bertujuan untuk membuat cadangan data. Sehingga, jika data yang tersedia rusak atau hilang, data tersebut dapat diakses kembali. Biasanya, data yang telah disalin, disimpan pada perangkat keras atau diupload ke dalam cloud.

Kegiatan *Backup* ditujukan sebagai DRP (*Disaster Recovery Planning*) dalam bisnis. DRP merupakan bagian perencanaan dari sebuah institusi untuk melakukan tahapan tertentu yang nantinya akan menjamin kelangsungan pelayanan (khususnya dari segi sistem informasi) yang

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 51 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

Standar Prosedur Operasional Pengelolaan Teknologi Informasi (TI)

Bab X Keamanan Data



diberikan tanpa mengurangi kapabilitas serta kinerja dari sebuah sistem jika terjadi sebuah bencana di dalamnya.

Hal ini sesuai dengan anjuran pemerintah dalam pasal 40 ayat (1) dan ayat (4) Perpres 95 tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) mewajibkan penyediaan cadangan (*Backup*) dan Pemulihan (*Restore*). Sehingga jika bisnis terkena bencana baik alam, terserang virus/*malware* atau bahkan perangkat rusak. *Backup* data menjadi kebutuhan wajib dari pemerintah demi keberlangsungan bisnis

Ada beberapa faktor atau alasan mengapa kebijakan *backup* data harus dilakukan diantaranya adalah:

1. Human Error

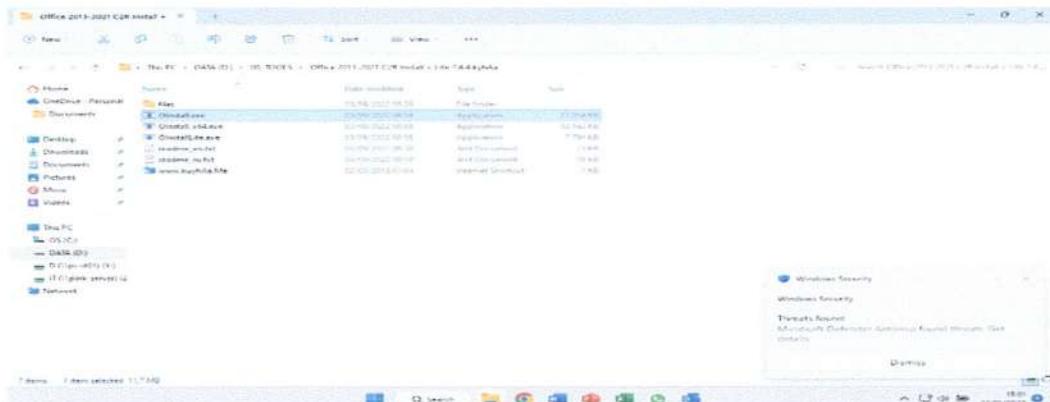
Human Error atau kelalaian Sumber Daya Manusia (SDM) merupakan kesalahan yang paling sering terjadi di industri manapun. Menurut survei dari sumber Mashable, Data Breach Infographic menyatakan bahwa 32% rusak dan hilangnya data disebabkan oleh Human Error. Umumnya, hal ini terjadi dikarenakan kurangnya fokus ketika kita bermaksud menghapus data yang sudah tidak diperlukan dan kesengajaan menghapus data/ partisi dan melakukan format *hard drive*.

2. Rusaknya Tools Penyimpanan

Menurut survei dari sumber Mashable, Data Breach Infographic menyatakan bahwa 21% data hilang dikarenakan kegagalan hardware, sistem *crash*, *software corrupt*. Saat ini, kehilangan data terKebanyakan orang menyimpan data mereka pada perangkat keras seperti HDD/ SSD. Perlu diketahui bahwa, perangkat keras selalu mempunyai risiko kerusakan yang mengakibatkan hilangnya data. Kerusakan tools dapat terjadi karena berbagai sebab, seperti kurangnya informasi mengenai bagaimana merawat perangkat keras dengan baik, terjadinya bencana alam, dan lain sebagainya.

3. Serangan Virus/*Malware*

Dalam survei sumber Mashable, Data Breach Infographic menjelaskan ketidaksengajaan seperti terserang virus atau *malware* atau bahkan situs diretas oleh oknum yang tidak bertanggung jawab. Serangan Virus merupakan salah satu penyebab umum hilang atau rusaknya suatu data. Serangan ini bisa terjadi kapan saja saat mengoperasikan perangkat seperti komputer, laptop, *smartphone* dan lainnya.



Notes : Notifikasi dari antivirus ketika terjadi serangan

Cara kerja virus sangatlah beragam, beberapa virus dapat merusak data dengan mengunci *file*, atau menghapus *file* dari perangkat. Beberapa virus juga dapat merusak perangkat keras dengan cara menggandakan data, hingga memenuhi kapasitas penyimpanan perangkat.

Backup data dapat dilakukan dengan menggunakan 3 cara yang paling umum. Berikut adalah jenis-jenis *backup* data yang dapat kamu gunakan:

- a. *Full Backup* – Membuat salinan semua data yang tersimpan ke dalam satu lokasi. *Backup* data ini dapat memakan waktu berjam-jam hingga berhari-hari tergantung pada banyaknya data yang disimpan.
- b. *Incremental Backup* – Penyalinan data baru sejak *backup* data terakhir dilakukan. Namun full *backup* perlu dilakukan terlebih dahulu sebelum melakukan incremental *backup* dilakukan untuk pertama kali. Setelah itu, sistem secara otomatis dapat melakukan incremental *backup* sesuai dengan tanggal dan waktu terakhir *backup* dilakukan.
- c. *Differential Backup* – Salinan semua data yang telah diubah dari proses *backup* sebelumnya. Differential *backup* akan terus melakukan penyalinan data yang diubah sejak proses *backup* sebelumnya selesai.

Pengujian data yang sudah dibackup perlu dilakukan dengan cara melakukan restore data yakni dengan proses pengembalian data dari file backup yang dilakukan saat terjadi kerusakan, kecelakaan, atau bencana alam yang merusak data utama.

D. Ketentuan Keamanan Penyalinan Data

Untuk melindungi data penting perusahaan, perlu dilakukan *backup* dan *recovery* data. *Backup* data dan *recovery* data adalah proses penyalinan data kemudian menyimpannya di lokasi alternatif yang aman sehingga data dapat dipulihkan kemudian. Ada beberapa jenis *recovery* data yang umum digunakan oleh perusahaan atau organisasi untuk melindungi data-data penting perusahaan. Jenis-jenis tersebut dapat kamu pilih untuk mengamankan data, diantaranya adalah:

1. *Virtual Recovery* – Didukung oleh portal visualisasi yang juga menghadirkan layanan *backup*. Seperti namanya, jenis *Recovery* ini menggunakan virtualisasi dalam proses pemulihan datanya. Pusat data virtual ditempatkan untuk menginstal *server* fisik sebagai perangkat utama.
2. Jaringan *Recovery* – Berpusat pada pemulihan jaringan. Prosedur ini melibatkan koneksi dengan anggota unit kerja TI, perangkat jaringan, serta sejumlah usaha lain yang terkait dengan koneksi yang terputus.
3. *Recovery Data Center* – Data center atau pusat data perusahaan ditempatkan dalam sebuah sistem khusus dengan fasilitas komputerisasi. Untuk melakukan *recovery* ini, pusat data perlu dikembangkan terlebih dahulu lewat prosedur penanganan lokasi, pemantapan perangkat dan pegawai, serta pengaturan HVAC ruangan (*Heating, Ventilation, Air Conditioning*).
4. *Recovery Data Berbasis Cloud* – Merupakan jenis *recovery* data yang paling populer. *Recovery* data menggunakan portal penyimpanan dan pemulihan data yang diatur layanan pihak ketiga. Dengan begitu, perusahaan tidak perlu mengembangkan fasilitas sendiri.

E. Ketentuan komputer seluler/ laptop dalam hal keamanan komputer (*Computer Security*)

Keamanan komputer (*Computer Security*) merupakan suatu cabang teknologi yang dikenal dengan nama keamanan informasi yang diterapkan pada komputer. Dalam rangka mengontrol penggunaan komputer seluler, terdapat beberapa hal yang dapat diterapkan antara lain:

1. Otentikasi untuk semua aplikasi
 - a. Memiliki otentikasi yang kuat untuk setiap aplikasi dan setiap pengguna secara signifikan mengurangi risiko pelanggaran. Lagi pula, kata sandi mudah dikompromikan.
 - b. Otentikasi multifaktor (MFA) menawarkan kontrol yang kuat bahkan ketika kata sandi disusupi. Sebagian besar perusahaan memiliki MFA, tetapi tidak diaktifkan untuk setiap aplikasi. Keamanan hanya sebagus tautan terlemah. Miliki peta jalan untuk mengaktifkan MFA untuk setiap permintaan *log in* di organisasi Anda.
 - c. Tidak ada pengecualian. Tentu saja, perusahaan dapat memanfaatkan kebijakan masuk tunggal dan autentikasi adaptif untuk menghindari masalah MFA bagi pengguna akhir. Anda dapat menantang pengguna untuk otentikasi hanya ketika sesuatu berubah atau ketika risikonya tinggi.
 - d. Faktor otentikasi yang Anda gunakan untuk MFA penting. Misalnya, kode sandi satu kali (OTP) yang dikirimkan melalui SMS tidak lagi dapat diandalkan karena peretas dapat mencurinya melalui teknik tipe man-in-the-middle atau dengan alat peretas untuk mengelabui pengguna agar mengungkapkan OTP. Tetap saja, itu lebih baik daripada tidak memiliki MFA.
2. Periksa perangkat pengguna sebelum beri akses
 - a. Mempertahankan sistem operasi dan browser terbaru untuk semua perangkat pengguna akhir menawarkan keuntungan terbesar bagi Anda. Microsoft, Apple, dan Google mengontrol sebagian besar sistem operasi dan browser dan sering merilis patch. Tim TI dan keamanan perlu memikirkan untuk memungkinkan pengguna akhir memelihara perangkat mereka.
 - b. Misalnya, Anda dapat memanfaatkan teknologi autentikasi yang memberi tahu pengguna akhir kapan mereka perlu memperbarui perangkat mereka. Perusahaan yang sadar akan keamanan memblokir perangkat agar tidak mengakses aplikasi penting jika perangkat tidak mutakhir.
3. Mengawasi aktivitas karyawan secara paripurna

Perusahaan juga dapat mengadopsi teknologi Data leak Prevention (DLP) Safetica untuk menetralisir segala macam ancaman keamanan, karena teknologi Safetica mengacu pada perlindungan data rahasia agar tidak bocor kepada pihak yang tidak berwenang, dengan memonitor data yang digunakan saat dipenyimpanan dan transit, dan mencegah pelanggaran data secara real time meskipun karyawan berada di luar perusahaan.

Enkripsi adalah proses mengacak data sehingga data hanya dapat dipahami oleh orang-orang tertentu saja. Secara teknis, enkripsi berarti proses mengubah plaintext-teks yang bisa dipahami manusia-, menjadi ciphertext yang tidak bisa dipahami.

Pengacakan data dalam enkripsi tidak benar-benar dilakukan secara acak. Dalam prosesnya, enkripsi menggunakan *cryptographic key*, yaitu string karakter dalam algoritma enkripsi yang dapat mengubah data menjadi acak.

Cryptographic key berisi sekumpulan nilai matematika yang disepakati oleh pengirim dan penerima pesan terenkripsi. Hal inilah yang menyebabkan data menjadi terkunci (*encryption*) namun dapat tetap dibuka (*decryption*) oleh pihak tertentu.

A. Manfaat Enkripsi

Teknologi encryption memiliki banyak manfaat dalam penggunaanya. Berikut ini adalah beberapa manfaatnya:

1. Menjaga privasi pengguna

Enkripsi bekerja dengan cara mengacak data menjadi tidak dapat dipahami oleh orang lain. Hal ini tentunya bertujuan untuk menjaga privasi pengguna data. Dengan data yang terenkripsi, masalah kebocoran privasi juga dapat dicegah dengan lebih baik.

2. Memberi perlindungan aplikasi saluran percakapan

Bayangkan jika semua orang dapat membaca chat pribadimu dengan seseorang. Selain kehilangan privasi, kamu mungkin juga akan kehilang data-data pribadimu. Untuk itu, enkripsi adalah komponen keamanan yang penting bagi aplikasi percakapan seperti WhatsApp, agar privasi penggunanya dapat selalu terjaga.

3. Digital signature

Selain menjaga privasi dan keamanan, enkripsi juga bisa dimanfaatkan sebagai digital signature. Digital signature sendiri merupakan suatu baris pernyataan pada e-copy seperti *email*, yang berisi pernyataan terenkripsi. Sehingga, hanya orang tertentu yang dapat memahami pernyataan tersebut setelah melakukan dekripsi.

B. Key Encryption

Enkripsi dibedakan dari *encryption key* yang digunakan, yaitu enkripsi simetris dan enkripsi asimetris. Berikut ini adalah penjelasan keduanya:

1. Enkripsi simetris

Symmetric enkripsi adalah jenis enkripsi yang proses penguncian data dan proses pembukaan datanya dilakukan menggunakan satu kunci yang sama.

Karena menggunakan satu kunci yang sama, maka algoritma enkripsi pada jenis ini terlihat tidak terlalu kompleks dan cenderung lebih mudah untuk dieksekusi. Jenis enkripsi ini adalah pilihan yang tepat untuk membawa transmisi data dalam jumlah besar.

2. Enkripsi asimetris

Enkripsi asimetris dikenal juga dengan *public-key cryptography* atau *public-key encryption*. Hal ini karena enkripsi jenis ini menggunakan dua kunci yang saling berhubungan, yaitu kunci publik dan kunci pribadi.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 55 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

Kunci publik berfungsi untuk mengenkripsi pesan dan dapat diakses oleh semua orang. Sedangkan kunci pribadi berfungsi untuk mendekripsi pesan dan hanya dapat diakses oleh pemilik kunci untuk menjaga privasi. Jenis enkripsi asimetris lebih kompleks dan memakan lebih banyak waktu. Tapi, keamanannya lebih kuat jika dibandingkan dengan enkripsi simetris.

C. Tipe Enkripsi

Selain dibedakan berdasarkan jenisnya, enkripsi juga memiliki beberapa tipe yang dilihat dari kebutuhan penggunaan, infrastruktur, maupun parameter lainnya.

1. *Encryption as a service* (EaaS), menyewakan enkripsi bagi pengguna dengan sumber daya yang sedikit dan tidak mampu membuat enkripsi sendiri. Pada enkripsi tipe ini, pengguna perlu mematuhi segala peraturan yang berlaku dan selalu menjaga data mereka di lingkungan penyewa.
2. *Bring your own encryption* (BYOE), enkripsi tipe ini cocok untuk pengguna layanan *cloud* yang ingin mengelola perangkat lunak dan kunci enkripsi mereka sendiri.
3. *Cloud storage encryption*, merupakan tipe enkripsi yang disediakan oleh penyedia layanan *cloud*. Mereka mengenkripsi data menggunakan algoritma dan penyimpanan mereka sendiri, sehingga pengguna hanya perlu menyewanya.
4. *Deniable encryption*, adalah tipe enkripsi yang memungkinkan data terenkripsi untuk didekripsi dalam dua cara atau lebih berdasarkan kunci enkripsi yang digunakan oleh suatu pihak
5. *Column-level encryption*, cocok digunakan untuk enkripsi basis data. Di mana setiap sel dalam kolom data tertentu dapat diakses dengan kata sandi yang sama.
6. *Field-level encryption*, enkripsi jenis ini mengelola suatu enkripsi data pada bidang tertentu dari halaman web. Misalnya, mengenkripsi nomor KTP, nomor kartu kredit, dll.
7. *End-to-end encryption* (E2EE), adalah tipe enkripsi yang banyak digunakan oleh aplikasi *chatting*. Enkripsi E2EE memastikan komunikasi antara dua pihak tidak dapat dibaca oleh pihak lain.
8. *Full-disk encryption* (FDE), enkripsi jenis ini bekerja pada tingkat *hardware* dan mengubah semua data pada disket menjadi bentuk yang tidak bisa dipahami. FDE hanya dapat diakses oleh orang tertentu yang memiliki kunci autentikasi.
9. *Network-level encryption*, merupakan tipe enkripsi yang mengandalkan jaringan internet melalui *Internet Protocol Security* (IPSec). Enkripsi tipe ini memastikan komunikasi yang aman di level transfer jaringan.
10. *Link-level encryption*, tipe enkripsi ini ada pada level tautan atau link. Di mana data dienkripsi saat dikirim dari host, dan didekripsi saat mencapai tautan selanjutnya.
11. *Hypertext Transfer Protocol Secure* ([HTTPS](https://)), mengenkripsi setiap konten yang dikirim oleh web server dan melakukan verifikasi apakah *public-key encryption* telah terinstall.
12. *Homomorphic encryption*, adalah tipe enkripsi yang mengubah data menjadi ciphertext yang dapat diproses, sehingga memungkinkan pengguna untuk melakukan operasi kompleks pada data yang terenkripsi.

**Standar Prosedur Operasional
Pengelolaan Teknologi Informasi (TI)**

Bab XI Key Encryption



D. Penerapan Enkripsi

Enkripsi adalah faktor penting dalam *cyberSecurity*. Setidaknya, ada beberapa penggunaan enkripsi yang dimanfaatkan untuk mendukung keamanan siber, seperti berikut ini:

1. *Enkripsi data*

Banyak perusahaan yang membutuhkan privasi dan keamanan data. Untuk itu, enkripsi seringkali digunakan untuk menjaga keamanan data mereka. Seperti *file database, warehouse, hingga backup server*.

2. *Enkripsi file*

Enkripsi dapat digunakan untuk mengamankan *file* yang bersifat penting dan rahasia, seperti *file* perusahaan yang ada di komputer maupun *cloud*. *File* tersebut nantinya akan dienkripsi dan hanya orang-orang tertentu saja yang dapat mendekripsinya.

3. *Encryption messaging*

Penggunaan enkripsi juga bisa kamu lihat dalam aplikasi perpesanan seperti *WhatsApp* dan *Telegram*. Agar pesanmu hanya bisa dibaca oleh orang yang bersangkutan, maka aplikasi perpesanan menggunakan *End-to-end encryption (E2EE)* untuk membuat privasinya tetap terjaga.

4. *Endpoint encryption*

Selain memasang antivirus, enkripsi adalah salah satu upaya bisa kamu gunakan untuk memberikan perlindungan pada operating *System* perangkatmu, seperti komputer, laptop, tablet, dll. Dengan enkripsi, beberapa serangan siber yang mengakses data secara ilegal pada perangkatmu akan lebih sulit untuk dilakukan.

Kontrol akses adalah bagian dari keamanan yang dialami orang pertama dan paling sering. Mereka melihatnya ketika mereka masuk ke komputer dan ponsel mereka, ketika mereka berbagi *file* atau mencoba mengakses aplikasi, dan ketika mereka menggunakan kunci kartu ID untuk memasuki gedung atau ruangan. Meskipun kontrol akses bukanlah segalanya dalam keamanan, itu sangat penting, dan itu membutuhkan perhatian yang tepat sehingga pengalaman pengguna dan jaminan keamanan benar.

A. Strategi kontrol akses:

1. Komprehensif dan konsisten.
2. Menerapkan prinsip-prinsip keamanan secara ketat di seluruh tumpukan teknologi.
3. Cukup fleksibel untuk memenuhi kebutuhan organisasi.

Strategi kontrol akses yang baik melampaui satu taktik atau teknologi. Ini membutuhkan pendekatan pragmatis yang mencakup teknologi dan taktik yang tepat untuk setiap skenario.

Kontrol akses modern harus memenuhi kebutuhan produktivitas organisasi, dan juga menjadi:

1. **Aman:** Secara eksplisit memvalidasi kepercayaan pengguna dan perangkat selama permintaan akses, menggunakan semua data dan telemetri yang tersedia. Konfigurasi ini membuat lebih sulit bagi penyerang untuk meniru pengguna yang sah tanpa terdeteksi. Selain itu, strategi kontrol akses harus fokus pada penghapusan eskalasi hak istimewa yang tidak sah, misalnya, memberikan hak istimewa yang dapat digunakan untuk mendapatkan hak istimewa yang lebih tinggi. Untuk informasi selengkapnya tentang melindungi akses istimewa, lihat Mengamankan akses istimewa.
2. **Konsisten:** Memastikan bahwa jaminan keamanan diterapkan secara konsisten dan mulus di seluruh lingkungan. Standar ini meningkatkan pengalaman pengguna dan menghapus peluang bagi penyerang untuk menyelinap masuk melalui kelemahan dalam implementasi kontrol akses terputus-putus atau sangat kompleks. Anda harus memiliki strategi kontrol akses tunggal yang menggunakan jumlah mesin kebijakan paling sedikit untuk menghindari inkonsistensi konfigurasi dan drift konfigurasi.
3. **Komprehensif:** Penegakan kebijakan akses harus dilakukan sedekat mungkin dengan sumber daya dan jalur akses. Konfigurasi ini meningkatkan cakupan keamanan, dan membantu keamanan sesuai dengan skenario dan harapan pengguna dengan lancar. Manfaatkan kontrol keamanan untuk data, aplikasi, identitas, jaringan, dan database untuk mendorong penegakan kebijakan lebih dekat dengan aset bisnis bernilai.
4. **Identitas-sentris:** Prioritaskan penggunaan identitas dan kontrol terkait bila tersedia. Kontrol identitas memberikan konteks yang kaya ke dalam permintaan akses, dan konteks aplikasi yang tidak tersedia dari lalu lintas jaringan mentah. Kontrol jaringan masih penting, dan kadang-kadang satu-satunya pilihan yang tersedia (seperti di lingkungan teknologi operasional), tetapi identitas harus selalu menjadi pilihan pertama jika tersedia. Dialog kegagalan selama akses aplikasi dari lapisan identitas akan lebih tepat dan informatif daripada blok lalu lintas jaringan, sehingga kemungkinan besar pengguna dapat memperbaiki masalah tanpa panggilan meja bantuan yang mahal.

**Standar Prosedur Operasional
Pengelolaan Teknologi Informasi (TI)**

Bab XII Kontrol Akses

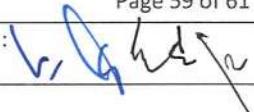


B. Model Akses Perusahaan

Model akses perusahaan adalah model akses komprehensif berdasarkan zero trust. Model ini membahas semua jenis akses oleh pengguna internal dan eksternal, layanan, aplikasi, dan akun istimewa dengan akses administratif ke sistem.

Salah satu perspektif yang bermanfaat tentang transformasi zero trust kontrol akses adalah bahwa ia bergeser dari proses autentikasi dan otorisasi dua langkah statis, ke proses tiga langkah dinamis yang disebut *dikenal, terpercaya, diizinkan*:

1. **Dikenal:** Autentikasi yang memastikan Anda adalah siapa yang Anda katakan. Proses ini *analog* dengan proses fisik memeriksa dokumen identifikasi foto yang dikeluarkan pemerintah.
2. **Terpercaya:** Validasi bahwa pengguna atau perangkat cukup dapat dipercaya untuk mengakses sumber daya. Proses ini *analog* dengan keamanan di bandara yang menyaring semua penumpang untuk risiko keamanan sebelum mengizinkan mereka memasuki bandara.
3. **Diizinkan:** Pemberian hak dan hak istimewa khusus untuk aplikasi, layanan, atau data. Proses ini *analog* dengan maskapai penerbangan yang mengelola ke mana penumpang akan pergi, kabin apa yang mereka duduki (kelas satu, kelas bisnis, atau pelatih), dan apakah mereka harus membayar bagasi.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 59 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

Standar Prosedur Operasional Pengelolaan Teknologi Informasi (TI)	 Bab XIII Analisa Manajemen Risiko
--	---

A. RISIKO DAN MITIGASI

Secara umum Mitigasi Risiko atas Ketentuan Vendor Management & Pengadaan Barang Jasa mengacu pada prinsip-prinsip Manajemen Risiko Operasional. Berdasarkan hasil identifikasi, terdapat risiko-risiko yang mungkin terjadi antara lain:

NO	KEJADIAN	PENYEBAB	MITIGASI	JENIS RISIKO	PENGENDALIAN
1.	<i>Server slow response</i>	Terindikasi virus <i>Malware</i> pada jaringan	Melakukan patroli <i>server-server</i> secara periodik setiap minggu	Operasional	<ul style="list-style-type: none"> - Investigasi running task yang tidak wajar - Pembuatan <i>Script CMD</i> untuk <i>task scheduler</i> yg dapat secara otomatis melakukan <i>end-task</i> program yang tidak wajar.
2.	<i>Windows problem</i>	Sistem Operasi Windows tidak di <i>update</i> atau di <i>skip</i>	Cek <i>Update OS Windows</i> setiap pagi hari	Operasional	<i>Update windows</i> dan <i>restart</i> kembali
3.	<i>Virus found</i>	Sistem Operasi Windows tidak di <i>update</i> atau di <i>skip</i>	Periksa <i>Update Virus Definitions</i> secara periodik	Operasional	Memperbarui secara berkala <i>Virus Definitions</i> dan <i>restart System</i> operasi
4.	Jaringan internet mati	<ul style="list-style-type: none"> - Device <i>overheat</i> - Gangguan jaringan internet dari provider - Kabel jaringan yang tidak tersambung / putus 	<ul style="list-style-type: none"> - Melakukan <i>restart</i> rutin pada <i>device</i> - Melakukan penggantian <i>device</i> yang sudah tidak layak pakai - Pengecekan jaringan internet secara berkala - Melakukan perawatan atau penggantian pada infrastruktur jaringan 	Operasional	<ul style="list-style-type: none"> - Melakukan <i>restart</i> pada <i>device</i> yang <i>overheat</i> atau jika rusak dilakukan penggantian yang baru - Mengajukan keluhan ke <i>customer care</i> provider untuk membuat tiket pengaduan agar segera ditindak - Melakukan <i>tracing</i> kabel untuk mencari posisi kabel yang putus / melakukan <i>crimping</i> ulang pada kabel yang tidak tersambung

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 60 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		

**Standar Prosedur Operasional
Pengelolaan Teknologi Informasi (TI)**

Bab XIII Analisa Manajemen Risiko



B. PENUTUP

1. Standar Prosedur Operasional (SPO) Pengelolaan Teknologi Informasi ini berlaku terhitung sejak diterbitkannya SPO ini.
2. Standar Prosedur Operasional ini akan di review secara berkala sekurang-kurangnya 2 (dua) tahun sekali dan akan dilakukan penyesuaian apabila terdapat hal-hal yang belum diatur atau karena adanya perubahan ketentuan eksternal / internal yang terkait.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 61 of 61
No Reg :	001/2023/SPO/RSC	Edisi : 02	Diverifikasi oleh :	
Tgl Berlaku :	27 Januari 2023	Revisi :		