



# **STANDAR PROSEDUR OPERASIONAL PENGELOLAAN TEKNOLOGI INFORMASI**

**NOMOR REGISTRASI: 004/2022/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)		24/11/22

**Dikaji oleh:**

Nama	Jabatan	Unit Kerja	Tanda Tangan	Tanggal
Reko Afiantoro	Manager IT Support	Risk, System & Compliance (RSC)		23/11/22
Endang Pariyanto	Manager Risk Management & Compliance			24/11/22
Eko Ervan	General Manager RSC			25/11/22
Haris Triyadi	Executive General Manager Finance & Support			26/Nov m.

**Disetujui oleh:**

Nama	Jabatan	Tanda Tangan	Tanggal
Hargo Hadi	Direktur Building, Construction & Support Management		28/11/2022
Sugeng Hariadi	Direktur Utama		28/11/22

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi	Halaman :
No Reg : 004/2022/SPO/RSC	Edisi :
Tgl Berlaku : <b>28/11/22</b>	Revisi : Diverifikasi oleh :

**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).

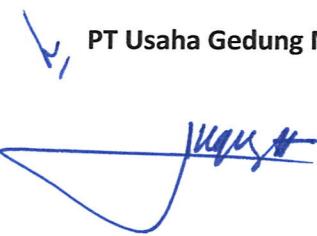
Setiap Pegawai PT UG Mandiri harus memahami, melaksanakan serta mematuhi isi SPO, sehingga diperoleh pemahaman tentang ketentuan dan pelaksanaan Pengelolaan Teknologi Informasi (IT Support).

SPO ini hanya boleh digunakan dalam lingkungan kantor PT UG Mandiri. Tidak diperkenankan untuk dicetak ulang, dicopy, 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, 28 November 2022

PT Usaha Gedung Mandiri

  
**Sugeng Hariadi**  
Direktur Utama

  
**Hargo Hadi**  
Direktur

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

**Daftar Isi**



Halaman

**KATA PENGANTAR**

i

**DAFTAR ISI**

1

Bab I.	<b>PENDAHULUAN</b>	
A.	Latar Belakang	2
B.	Maksud dan Tujuan	2
C.	Dasar Penyusunan	2
D.	Ruang Lingkup	3
E.	Daftar Istilah	3
Bab II. <b>ORGANISASI IT SUPPORT</b>		
A.	Organisasi Satuan Kerja IT Support	5
B.	Struktur Organisasi	5
1.	Satuan Kerja yang menangani Pengembangan Aplikasi IT	6
2.	Satuan Kerja yang menangani Operasional dan Infrastruktur TI	6
3.	Satuan Kerja yang menangani Keamanan Sistem Informasi TI	7
4.	Satuan Kerja yang menangani Media Social	7
C.	Evaluasi Organisasi IT Support	7
Bab III. <b>TATA KELOLA TEKNOLOGI INFORMASI</b>		
A.	Penyelenggaraan dan Pengelolaan Teknologi Informasi	9
B.	Wewenang	9
C.	Tanggung Jawab	10
D.	Pegawai/ User	10
E.	Komputer dan Hak Akses	10
F.	Aset Perusahaan	11
G.	Keamanan Server	11
H.	Keamanan <i>Hardware</i>	11
I.	Keamanan Jaringan Komunikasi Komputer dan Aplikasi Terapan	11
J.	Ketentuan Aplikasi Terapan Perusahaan	11
K.	Larangan	12
L.	Sanksi	12
Bab IV. <b>KETAHANAN SIBER</b>		
A.	Jenis Ancaman Siber	13
B.	Bentuk Ancaman Siber	13
C.	Penanggulangan Serangan Siber	15
Bab V. <b>ANALISA MANAJEMEN RISIKO</b>		
A.	Risiko dan Mitigasi	17
B.	Penutup	18

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

**Bab I Pendahuluan**



**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 asset 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. SPO No.002/2020/SPO/HCG perihal Tata Tertib dan Kedisiplinan Pegawai.
4. Pedoman Sistem Anti Penyuapan PT Usaha Gedung Mandiri No.UG/SMAP/PSMAP/002 tanggal 19 Agustus 2022.

**D. Ruang Lingkup**

Pengeloaan *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

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 2 of 18
No Reg :	004/2022/SPO/RSC	Edisi :	Diverifikasi oleh :	
Tgl Berlaku :	28/11/22,	Revisi :		

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

**Bab I Pendahuluan**



Logistik.

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 Aplikasi* : 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 3 of 18
No Reg :	004/2022/SPO/RSC	Edisi :	Diverifikasi oleh :	
Tgl Berlaku :	28/11/22	Revisi :		

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

**Bab I Pendahuluan**



XMMS, Realplayer, PowerDVD, dll.

14. *Software Jaringan* Aplikasi : Perangkat lunak yang digunakan untuk operasional di jaringan komputer 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 kedalam jaringan teknologi informasi.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 4 of 18
No Reg :	004/2022/SPO/RSC	Edisi :	Diverifikasi oleh :	
Tgl Berlaku :	. 28/11/22 .	Revisi :		

# Standar Prosedur Operasional Pengelolaan Teknologi Informasi (TI)

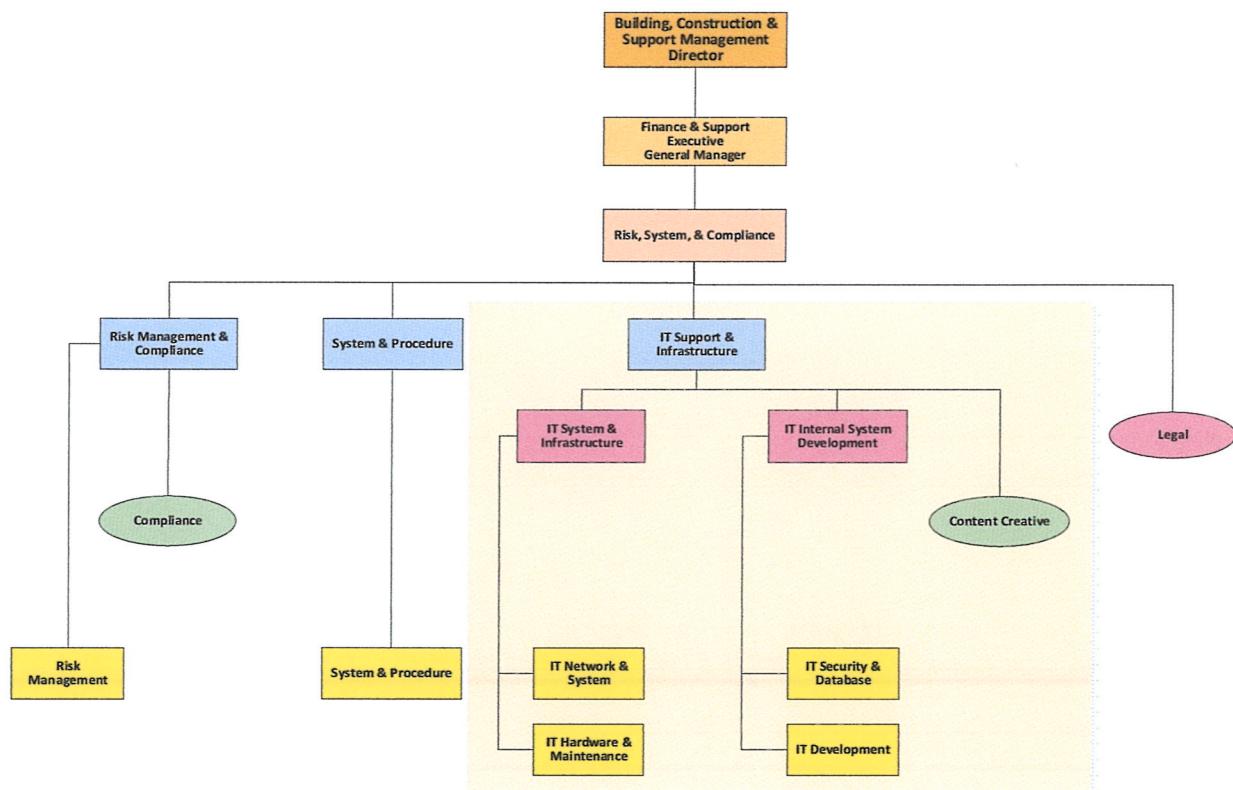
## Bab II Organisasi Pengelolaan TI



### A. Organisasi Satuan Kerja IT

1. Organisasi 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 TI yang digunakan di lingkungan Perusahaan.
2. 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)
3. Wewenang dan Tanggung Jawab Satuan Kerja IT Support mengacu pada Struktur Organisasi dan Tata Kerja Perusahaan yang berlaku.

### B. Struktur Organisasi



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

**Bab II Organisasi Pengelolaan TI**



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 6 of 18
No Reg :	004/2022/SPO/RSC	Edisi :	Diverifikasi oleh :	
Tgl Berlaku :	28/11/22.	Revisi :		

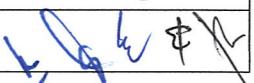
- e. Mengelola dan memberikan persetujuan terhadap *Go-Live checklist* untuk menentukan *release* sistem internal (*Deployment* pada aplikasi baru/perubahan, *patching*/ perubahan data, perubahan konfigurasi perangkat).
3. Satuan Kerja yang menangani Keamanan Sistem Informasi TI
  - a. Menyusun dan mengelola desain arsitektur keamanan sistem informasi dan mengajukan *enhancement* yang diperlukan dengan menimbang trend 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 *messanger (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 7 of 18
No Reg :	004/2022/SPO/RSC	Edisi :	Diverifikasi oleh :	
Tgl Berlaku :	28/11/22.	Revisi :		

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

**Bab II Organisasi Pengelolaan TI**



- 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.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 8 of 18
No Reg :	004/2022/SPO/RSC	Edisi :	Diverifikasi oleh :	
Tgl Berlaku :	28/11/22.	Revisi :		

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

**Bab III Tata Kelola Teknologi Informasi**



**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 social* 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 9 of 18
No Reg :	004/2022/SPO/RSC	Edisi :	Diverifikasi oleh :	
Tgl Berlaku :	28/11/22,	Revisi :		

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

**Bab III Tata Kelola Teknologi Informasi**



- i. Mencari dan mengusulkan konsultan teknologi informasi kepada Direksi untuk perencanaan, pengadaan, pembangunan dan pemeriksaan kualitas *hardware, software*, dan Teknologi Informasi yang tergolong spesifik.
- j. 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 10 of 18
No Reg :	004/2022/SPO/RSC	Edisi :	Diverifikasi oleh :	
Tgl Berlaku :	28/11/22.	Revisi :		

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

**Bab III Tata Kelola Teknologi Informasi**



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 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.

**J. 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.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 11 of 18
No Reg :	004/2022/SPO/RSC	Edisi :	Diverifikasi oleh :	
Tgl Berlaku :	28/11/22	Revisi :		

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

**Bab III Tata Kelola Teknologi Informasi**



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.

**K. 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.

**L. 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.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 12 of 18
No Reg :	004/2022/SPO/RSC	Edisi :	Diverifikasi oleh :	
Tgl Berlaku :	28/11/22,	Revisi :		

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

**Bab IV Ketahanan Siber**



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 13 of 18
No Reg :	004/2022/SPO/RSC	Edisi :	Diverifikasi oleh :	
Tgl Berlaku :	28/11/22.	Revisi :		

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

**Bab IV Ketahanan Siber**



**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***

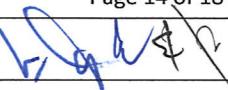
*Hacking* adalah kegiatan menerobos program komputer milik pihak lain. Biasanya, *hacker* akan mengambil alih sistem jaringan, akun sosial media, akun perbankan, mencuri data, dan lainnya.

**9. *Cross-Site Scripting (XSS)***

Sebuah jenis injeksi berupa *script* berbahaya yang diinjeksikan ke sebuah situs rentan maupun tepercaya. *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 14 of 18
No Reg :	004/2022/SPO/RSC	Edisi :	Diverifikasi oleh :	
Tgl Berlaku :	28/11/22,	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 beresiko untuk mengalami kebocoran data internal.

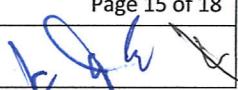
**C. Penanggulangan Serangan Siber**

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 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 15 of 18
No Reg :	004/2022/SPO/RSC	Edisi :	Diverifikasi oleh :	
Tgl Berlaku :	28/11/22.	Revisi :		

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

**Bab IV Ketahanan Siber**



- 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.

Standar Prosedur Operasional – Pengelolaan Teknologi Informasi			Halaman :	Page 16 of 18
No Reg :	004/2022/SPO/RSC	Edisi :	Diverifikasi oleh :	
Tgl Berlaku :	28/11/22,	Revisi :		

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

**Bab V 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 server-server secara periodik setiap minggu	Operasional	- 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	Update <i>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"> <li>- Device <i>overheat</i></li> <li>- Gangguan jaringan internet dari provider</li> <li>- Kabel jaringan yang tidak tersambung / putus</li> </ul>	<ul style="list-style-type: none"> <li>- Melakukan <i>restart</i> rutin pada <i>device</i></li> <li>- Melakukan penggantian <i>device</i> yang sudah tidak layak pakai</li> <li>- Pengecekan jaringan internet secara berkala</li> <li>- Melakukan perawatan atau penggantian pada infrastruktur jaringan</li> </ul>	Operasional	<ul style="list-style-type: none"> <li>- Melakukan <i>restart</i> pada <i>device</i> yang <i>overheat</i> atau jika rusak dilakukan penggantian yang baru</li> <li>- Mengajukan keluhan ke <i>customer care</i> provider untuk membuat tiket pengaduan agar segera ditindak</li> <li>- Melakukan <i>tracing</i> kabel untuk mencari posisi kabel yang putus / melakukan <i>crimping</i> ulang pada kabel yang tidak tersambung</li> </ul>

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

**Bab V 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 18 of 18
No Reg :	004/2022/SPO/RSC	Edisi :	Diverifikasi oleh :	
Tgl Berlaku :	28/11/22.	Revisi :		