

CYBER SECURITY

Bagian 1: Pedoman Umum Sistem Manajemen Pengamanan Data dan Informasi



PLN

PT PLN (Persero)
Jl. Trunojoyo Blok M-1/135 Kebayoran Baru
Jakarta Selatan 12160

CYBER SECURITY

Bagian 1: Pedoman Umum Sistem Manajemen Pengamanan Data dan Informasi



PLN

PT PLN (Persero)
Jl. Trunojoyo Blok M-1/135 Kebayoran Baru
Jakarta Selatan 12160

©PT PLN (Persero) 2024

Hak cipta dilindungi undang-undang. Dilarang menyalin atau menggandakan sebagian atau seluruh isi dokumen ini dengan cara dan dalam bentuk apapun dan dilarang mendistribusikan dokumen ini baik secara elektronik maupun tercetak di luar internal PLN tanpa izin tertulis dari PT PLN (Persero).

PT PLN (Persero)
Jl. Trunojoyo Blok M-1/135 Kebayoran Baru
Jakarta Selatan 12160

CYBER SECURITY

Bagian 1: Pedoman Umum Sistem Manajemen Pengamanan Data dan Informasi

Disusun oleh:

**Kelompok Bidang Standardisasi SCADA dan OPSIS
dengan Keputusan Direksi PT PLN (Persero)
No. 0053.K/DIR/2024**

**Kelompok Kerja Standardisasi
Cyber Security
dengan Keputusan General Manager
PT PLN (Persero) Puslitbang Ketenagalistrikan
No. 0065.K/GM-PUSLITBANG/2023**

Diterbitkan oleh :

**PT PLN (Persero)
JI. Trunojoyo Blok M - 1/135, Kebayoran Baru
Jakarta Selatan 12160**



PT PLN (PERSERO)

KEPUTUSAN DIREKSI PT PLN (PERSERO)

NOMOR: 0184 .K/DIR/2024

TENTANG

PENETAPAN SPLN S5.008-1: 2024
CYBER SECURITY BAGIAN 1: PEDOMAN UMUM SISTEM MANAJEMEN
PENGAMANAN DATA DAN INFORMASI

DIREKSI PT PLN (PERSERO)

Menimbang : a. bahwa untuk memberikan pedoman yang terarah dan seragam di lingkungan PT PLN (Persero) dalam pemilihan spesifikasi transformator tenaga pada jaringan tenaga listrik, maka Draf Standar Final (DSF) S5.008-1: 2024 yang disusun oleh Kelompok Standardisasi Bidang SCADA dan OPSIS perlu ditetapkan menjadi SPLN;

- b. bahwa Draf Standar Final (DSF) sebagaimana dimaksud pada huruf a telah memenuhi syarat untuk ditetapkan menjadi SPLN S5.008-1: 2024 *Cyber Security* Bagian 1: Pedoman Umum Sistem Manajemen Pengamanan Data dan Informasi ;
- c. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a dan b di atas, perlu ditetapkan Keputusan Direksi PT PLN (Persero) tentang Penetapan SPLN S5.008-1: 2024 *Cyber Security* Bagian 1: Pedoman Umum Sistem Manajemen Pengamanan Data dan Informasi .

Mengingat : 1. Undang-Undang Republik Indonesia Nomor 19 Tahun 2003 tentang Badan Usaha Milik Negara;

2. Undang-Undang Republik Indonesia Nomor 40 Tahun 2007 tentang Perseroan Terbatas;

3. Undang-Undang Republik Indonesia Nomor 30 Tahun 2009 tentang Ketenagalistrikan;

4. Undang-Undang Republik Indonesia Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Republik Indonesia Nomor 2 Tahun 2022 tentang Cipta Kerja menjadi Undang-Undang;

5. Peraturan...

Paraf

Lydia Ting



PLN

5. Peraturan Pemerintah Republik Indonesia Nomor 23 Tahun 1994 tentang Pengalihan Bentuk Perusahaan Umum (Perum) Listrik Negara Menjadi Perusahaan Perseroan (Persero);
6. Peraturan Pemerintah Republik Indonesia Nomor 45 Tahun 2005 tentang Pendirian, Pengurusan, Pengawasan dan Pembubaran Badan Usaha Milik Negara sebagaimana telah diubah dengan Peraturan Pemerintah Republik Indonesia Nomor 23 Tahun 2022;
7. Peraturan Pemerintah Republik Indonesia Nomor 14 Tahun 2012 tentang Kegiatan Usaha Penyediaan Tenaga Listrik sebagaimana telah diubah dengan Peraturan Pemerintah Republik Indonesia Nomor 23 Tahun 2014;
8. Peraturan Pemerintah Republik Indonesia Nomor 62 Tahun 2012 tentang Usaha Jasa Penunjang Tenaga Listrik;
9. Peraturan Pemerintah Republik Indonesia Nomor 25 Tahun 2021 tentang Penyelenggaraan Bidang Energi dan Sumber Daya Mineral;
10. Anggaran Dasar PT PLN (Persero);
11. Keputusan Menteri Badan Usaha Milik Negara Selaku Rapat Umum Pemegang Saham Perusahaan Perseroan (Persero) PT Perusahaan Listrik Negara Nomor SK-325/MBU/12/2019 tentang Pemberhentian, Perubahan Nomenklatur dan Pengangkatan Anggota-Anggota Direksi Perusahaan Perseroan (Persero) PT Perusahaan Listrik Negara;
12. Keputusan Menteri Badan Usaha Milik Negara Selaku Rapat Umum Pemegang Saham Perusahaan Perseroan (Persero) PT Perusahaan Listrik Negara Nomor SK-200/MBU/06/2021 tentang Pemberhentian, Pengalihan Tugas, dan Pengangkatan Anggota-Anggota Direksi Perusahaan Perseroan (Persero) PT Perusahaan Listrik Negara;
13. Keputusan Menteri Badan Usaha Milik Negara Selaku Rapat Umum Pemegang Saham Perusahaan Perseroan (Persero) PT Perusahaan Listrik Negara Nomor SK-389/MBU/12/2021 tentang Pemberhentian, Perubahan Nomenklatur Jabatan, dan Pengalihan Tugas Anggota-Anggota Direksi Perusahaan Perseroan (Persero) PT Perusahaan Listrik Negara;
14. Keputusan Menteri Badan Usaha Milik Negara Selaku Rapat Umum Pemegang Saham Perusahaan Perseroan (Persero) PT Perusahaan Listrik Negara Nomor SK-392/MBU/12/2021 tentang Pemberhentian dan Pengangkatan Anggota-Anggota Direksi Perusahaan Perseroan (Persero) PT Perusahaan Listrik Negara;

15. Keputusan...

Paraf

[Handwritten signature]



15. Keputusan Menteri Badan Usaha Milik Negara Selaku Rapat Umum Pemegang Saham Perusahaan Perseroan (Persero) PT Perusahaan Listrik Negara Nomor SK-2/MBU/01/2022 tentang Pemberhentian dan Pengangkatan Anggota Direksi Perusahaan Perseroan (Persero) PT Perusahaan Listrik Negara;
16. Keputusan Menteri Badan Usaha Milik Negara Selaku Rapat Umum Pemegang Saham Perusahaan Perseroan (Persero) PT Perusahaan Listrik Negara Nomor SK-162/MBU/07/2022 tentang Pemberhentian, dan Pengangkatan Anggota Direksi Perusahaan Perseroan (Persero) PT Perusahaan Listrik Negara;
17. Keputusan Menteri Badan Usaha Milik Negara Selaku Rapat Umum Pemegang Saham Perusahaan Perseroan (Persero) PT Perusahaan Listrik Negara Nomor SK-213/MBU/09/2022 tentang Pemberhentian, Perubahan Nomenklatur Jabatan, Pengalihan Tugas dan Pengangkatan Anggota-Anggota Direksi Perusahaan Perseroan (Persero) PT Perusahaan Listrik Negara;
18. Keputusan Menteri Badan Usaha Milik Negara Selaku Rapat Umum Pemegang Saham Perusahaan Perseroan (Persero) PT Perusahaan Listrik Negara Nomor SK-258/MBU/09/2023 tentang Pengangkatan Anggota Direksi Perusahaan Perseroan (Persero) PT Perusahaan Listrik Negara;
19. Keputusan Direksi PT PLN (Persero) Nomor 033.K/DIR/2005 tentang Penetapan PT PLN (Persero) Penelitian dan Pengembangan Ketenagalistrikan sebagai Penanggung Jawab Kegiatan Standardisasi di Lingkungan PT PLN (Persero);
20. Keputusan Direksi PT PLN (Persero) Nomor 304.K/DIR/2009 tentang Batasan Kewenangan Pengambilan Keputusan di Lingkungan PT PLN (Persero) sebagaimana telah beberapa kali diubah, terakhir dengan Peraturan Direksi PT PLN (Persero) Nomor 0297.P/DIR/2016;
21. Keputusan Direksi PT PLN (Persero) Nomor 0053.K/DIR/2024 tentang Pembentukan Kelompok Bidang Standardisasi Ketenagalistrikan di Lingkungan PT PLN (Persero);
22. Peraturan Direksi PT PLN (Persero) Nomor 0026.P/DIR/2024 tentang Organisasi dan Tata Kerja PT PLN (Persero).

MEMUTUSKAN:

Menetapkan : KEPUTUSAN DIREKSI PT PLN (PERSERO) TENTANG PENETAPAN SPLN S5.008-1: 2024 CYBER SECURITY BAGIAN 1: PEDOMAN UMUM SISTEM MANAJEMEN PENGAMANAN DATA DAN INFORMASI.

PERTAMA ...

Paraf

[Handwritten signature]



- PERTAMA : Menetapkan SPLN S5.008-1: 2024 *Cyber Security* Bagian 1: Pedoman Umum Sistem Manajemen Pengamanan Data dan Informasi sebagaimana tercantum dalam Lampiran Keputusan ini.
- KEDUA : SPLN S5.008-1: 2024 sebagaimana dimaksud dalam Diktum PERTAMA diberlakukan di lingkungan PT PLN (Persero) dan Anak Perusahaan PT PLN (Persero) melalui adopsi secara langsung oleh Direksi Anak Perusahaan atau pengukuhan dalam Rapat Umum Pemegang Saham (RUPS) Anak Perusahaan PT PLN (Persero).
- KETIGA : Pada saat Keputusan ini mulai berlaku, ketentuan-ketentuan lain yang bertentangan dengan Keputusan ini dicabut dan dinyatakan tidak berlaku.

Keputusan ini mulai berlaku terhitung sejak tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 14 Agustus 2024

DIREKTUR UTAMA,
DIREKSI
(persero)
DARMAWAN PRASODJO

Paraf *ky ddk Tg u gh*

Susunan Kelompok Bidang Standardisasi SCADA dan OPSIS

Surat Keputusan Direksi PT PLN (Persero)

No. 0053.K/DIR/2024

1. Agus Harya Maulana, S.T., M.T. : Sebagai Ketua merangkap Anggota
2. Guntur Supriyadi, S.T., M.Sc. : Sebagai Sekretaris merangkap Anggota
3. Arham, S.T., M.T. : Sebagai Anggota
4. Tri Hardimasyar, S.T., M.Sc. : Sebagai Anggota
5. Dr. Dhany Hermeidy Barus, S.T., M.T. : Sebagai Anggota
6. M. Chaliq Fadli, S.T., M.Sc. : Sebagai Anggota
7. Lugito Nurwahono, S.T., M.T. : Sebagai Anggota
8. Teguh Kurnianto, S.T. : Sebagai Anggota
9. M. Said Al Manshury, S.T., M.T. : Sebagai Anggota
10. Indra Utama Ichsan, S.T., M.M. : Sebagai Anggota
11. Doni Adrean, S.T. : Sebagai Anggota
12. Eko Wibowo, S.T., M.M. : Sebagai Anggota
13. Timbul Ferdinand S., S.T., M.T. : Sebagai Anggota
14. Popi Puspitasari, S.T., M.Sc. : Sebagai Anggota
15. Drie Alsi Laksana, S.T. : Sebagai Anggota
16. Elvanto Yanuar Ichsan, S.T., M.Sc. : Sebagai Anggota
17. Hendrix Reza, S.T. : Sebagai Anggota
18. H. M. Afip Nurul Hudah, S.T., M.T. : Sebagai Anggota

Susunan Kelompok Kerja Standardisasi CYBER SECURITY

Surat Keputusan General Manager PT PLN (Persero) Puslitbang Ketenagalistrikan
No. 0065.K/GM-PUSLITBANG/2023

- | | |
|---------------------------------------|--|
| 1. Eko Wibowo, S.T., M.M. | : Sebagai Ketua merangkap Anggota |
| 2. Ir. Kemas M. Tofani HS, S.T., M.T. | : Sebagai Sekretaris merangkap Anggota |
| 3. I Gusti Ngurah Eka, S.T. | : Sebagai Anggota |
| 4. Arief Basuki, S.T., M.T. | : Sebagai Anggota |
| 5. Agus Harya Maulana, S.T., M.T. | : Sebagai Anggota |
| 6. Teguh Kurnianto, S.T. | : Sebagai Anggota |
| 7. Erwan Kurniawan, S.T. | : Sebagai Anggota |
| 8. Axizis Pujie Irfanto, S.T. | : Sebagai Anggota |
| 9. Titi Okvita Dewi, S.T. , M.T. | : Sebagai Anggota |
| 10. Putu Ari Suyasa, S.T.. | : Sebagai Anggota |
| 11. Muhammad Husni Mubarak, S.T. | : Sebagai Anggota |
| 12. Haris Matinu Triyanto, S.T. | : Sebagai Anggota |

Daftar Isi

Daftar Isi	iii
Prakata	vii
1 Ruang lingkup	1
2 Tujuan	1
3 Acuan normatif	1
4 Istilah dan definisi.....	2
5 Fungsi dan peran organisasi keamanan data dan informasi.....	4
5.1 Peran dan tanggung jawab keamanan data dan informasi	4
5.2 Pemisahan wewenang	6
6 <i>Mobile device</i> dan <i>teleworking</i>	7
6.1 Kebijakan <i>mobile device</i>	7
6.2 Kebijakan <i>teleworking</i>	8
7 Keamanan sumber daya manusia	9
7.1 Sebelum masa kerja.....	9
7.1.1 Pemeriksaan latar belakang	9
7.1.2 Syarat dan ketentuan pekerjaan	9
7.2 Selama masa kerja.....	10
7.2.1 Tanggung jawab manajemen PLN.....	10
7.2.2 Evaluasi Kinerja.....	10
7.2.3 Kesadaran, edukasi, dan pelatihan keamanan data dan informasi	10
7.2.4 Tindakan kedisiplinan	11
7.3 Pemutusan dan perubahan kerja.....	12
7.3.1 Tanggung jawab pemutusan dan perubahan kerja	12
8 Manajemen aset.....	12
8.1 Tanggung jawab untuk aset	12
8.1.1 Pengadaan aset	12
8.1.2 Inventaris aset	12
8.1.3 Klasifikasi dan pelabelan/identifikasi aset	13
8.1.4 Kepemilikan aset	13
8.1.5 <i>Acceptable use of asset</i>	13
8.1.6 Pengelolaan dan pemeliharaan aset.....	13
8.1.7 Pengembalian aset.....	14
8.1.8 Penghapusan aset.....	14
8.2 Klasifikasi informasi.....	14
8.3 Penanganan media penyimpanan data dan informasi	15
9 Kontrol akses	16

9.1	Kebutuhan bisnis atas kontrol akses.....	16
9.1.1	Kebijakan kontrol akses	16
9.1.2	Akses ke jaringan dan layanan jaringan	18
9.1.3	Kebijakan penggunaan layanan jaringan.....	18
9.2	Manajemen akses <i>user</i>	19
9.3	Tanggung jawab <i>user</i>	22
9.3.1	Penggunaan <i>password</i>	22
9.4	Kontrol akses sistem dan aplikasi	23
9.4.1	Pembatasan akses informasi	23
9.4.2	Prosedur <i>log on</i> secara aman	23
9.4.3	Sistem manajemen <i>password</i>	23
9.4.4	Pemakaian program <i>utility</i>	24
9.4.5	Akses ke kode program (<i>source code</i>)	24
10	Kriptografi	24
10.1	Kontrol kriptografi.....	24
10.1.1	Kebijakan penggunaan kontrol kriptografi.....	24
10.1.2	Manajemen <i>key</i> (kriptografi)	25
10.1.3	Dukungan manajemen atas penerapan kriptografi	26
11	Keamanan fisik dan lingkungan	26
11.1	Secure area	26
11.1.1	Keamanan perimeter fisik.....	26
11.1.2	Kontrol akses masuk.....	27
11.1.3	Pengamanan kantor, ruangan, fasilitas di secure area.....	27
11.1.4	Pengamanan terhadap bencana	28
11.1.5	Bekerja di secure area	29
11.2	Peralatan	29
11.2.1	Keamanan dan penempatan peralatan	29
11.2.2	Peralatan listrik cadangan	30
11.2.3	Keamanan perkabelan	30
11.2.4	Pemeliharaan peralatan	30
11.2.5	Pemindahan peralatan	31
11.2.6	Keamanan peralatan dan aset di luar lokasi.....	32
11.2.7	Pemusnahan atau penggunaan kembali peralatan secara aman	32
11.2.8	Peralatan tanpa pengawasan.....	32
11.2.9	Kebijakan <i>clean desk</i> dan <i>clear screen</i>	32
12	Keamanan operasional	33
12.1	Prosedur dan tanggung jawab operasional	33
12.1.1	Dokumentasi prosedur operasional.....	33
12.1.2	Manajemen perubahan	34

12.1.3	Manajemen kapasitas.....	35
12.1.4	Pemisahan lingkungan pengembangan, pengujian, dan operasional.....	35
12.2	Pengamanan dari <i>malware</i>	36
12.2.1	Kontrol terhadap <i>malware</i>	36
12.3	<i>Backup</i>	37
12.3.1	<i>Backup</i> data dan informasi	37
12.3.2	Pengujian berkala <i>backup</i>	37
12.3.3	Penjadwalan <i>backup</i>	37
12.3.4	<i>Backup off-site</i>	37
12.3.5	Persyaratan minimum penyimpanan <i>backup</i>	37
12.3.6	Perlindungan <i>backup</i>	37
12.4	Pencatatan <i>log</i> dan <i>monitoring</i>	38
12.4.1	<i>Monitoring</i> atas <i>log</i> penggunaan internet.....	38
12.4.2	Pencatatan <i>log</i> kejadian	38
12.4.3	Perlindungan atas <i>log</i>	38
12.4.4	<i>Log</i> administrator dan operator.....	38
12.4.5	<i>Review log</i>	38
12.4.6	Sinkronisasi waktu	38
12.5	Kontrol atas <i>software</i> operasional	39
12.5.1	Instalasi <i>software</i> pada sistem operasional.....	39
12.6	Kerentanan teknis	39
12.6.1	Pengendalian kerentanan teknis.....	39
12.6.2	Pembatasan instalasi <i>software</i>	39
12.7	Pertimbangan audit sistem data dan informasi	40
12.7.1	Kontrol audit sistem data dan informasi	40
13	Keamanan komunikasi	40
13.1	Manajemen keamanan jaringan	40
13.1.1	Kontrol jaringan	40
13.1.2	Keamanan layanan jaringan	42
13.1.3	Pemisahan jaringan	43
13.1.4	Dokumentasi jaringan	43
13.2	Transfer data dan informasi.....	43
13.2.1	Kebijakan dan prosedur keamanan transfer data dan informasi	43
13.2.2	Ketentuan transfer data dan informasi	44
13.2.3	Pesan elektronik	45
13.2.4	Perjanjian kerahasiaan (<i>non-disclosure agreement</i>)	47
14	Akuisisi, pengembangan dan pengelolaan sistem informasi.....	48
14.1	Kebutuhan keamanan sistem informasi.....	48
14.1.1	Analisis dan spesifikasi kebutuhan keamanan data dan informasi	48

14.1.2 Pengamanan layanan aplikasi pada jaringan publik	49
14.1.3 Pengamanan transaksi layanan aplikasi	49
14.2 Keamanan dalam proses pengembangan.....	49
14.2.1 Kebijakan keamanan dalam pengembangan.....	49
14.2.2 Prosedur kontrol pengembangan dan perubahan sistem	50
14.2.3 Review teknikal setelah perubahan <i>platform</i>	52
14.2.4 Pembatasan perubahan pada <i>software package</i>	52
14.2.5 Prinsip keamanan pengembangan sistem.....	53
14.2.6 Keamanan lingkungan pengembangan	53
14.2.7 Pengembangan perangkat lunak oleh mitra kerja.....	54
14.2.8 Pengujian keamanan sistem	55
14.2.9 <i>System acceptance testing</i>	55
14.2.10 Pengelolaan dan pemeliharaan perangkat lunak.....	55
14.3 Data pengujian.....	55
14.3.1 Perlindungan data pengujian.....	55
15 Kerjasama dengan mitra kerja	56
15.1 Keamanan dalam kerjasama mitra kerja	56
15.1.1 Kebijakan keamanan dalam kerjasama mitra kerja	56
15.1.2 Perjanjian keamanan dengan mitra kerja	56
15.1.3 Persyaratan keamanan dalam <i>supply chain</i>	57
15.2 Manajemen mitra kerja	57
15.2.1 Pengawasan dan <i>review</i> layanan mitra kerja	57
15.2.2 Hak audit atas mitra kerja.....	57
15.2.3 Manajemen perubahan terhadap layanan mitra kerja.....	58
16 Keamanan data dan informasi dalam manajemen keberlangsungan bisnis	58
16.1 Keberlangsungan keamanan data dan informasi	58
16.1.1 Keamanan data dan informasi dalam <i>business continuity management</i> (BCM)	58
16.1.2 <i>Business continuity plan</i> (BCP)	58
16.1.3 Implementasi keberlangsungan keamanan data dan informasi	58
16.2 Redundansi	60
16.2.1 Ketersediaan fasilitas pemrosesan informasi	60
17 Kepatuhan	61
17.1 Audit keamanan data dan informasi.....	61
17.1.1 Audit independen terhadap keamanan data dan informasi.....	61
17.1.2 Kepatuhan dengan kebijakan dan standar keamanan.....	61
17.1.3 Review kepatuhan.....	62
17.1.4 Pengamanan data rekaman	63

Prakata

Standar ini merupakan pedoman yang mengatur terkait keamanan siber (*cyber security*) dilingkungan PLN *group*. Mulai dari sisi *hardware*, manuasi, proses, kebijakan, peran, dan tanggung jawab hingga sisi *software*.

SPLN *cyber security* merupakan upaya kolaboratif untuk menyelami kompleksitas tantangan keamanan siber yang dihadapi oleh PLN dalam menjalankan fungsi operasinya sebagai penyedia energi di Indonesia. Standar ini diharapkan dapat memberikan solusi yang seragam untuk melindungi infrastruktur kritis dan data serta informasi yang menjadi nyawa operasional perusahaan.

Standar ini dapat dijadikan sebagai pedoman PLN pusat, unit induk, dan unit pelaksana dalam mengimplementasikan *cyber security* dilingkungan PLN *group*.

SPLN *cyber security* ini akan terdiri dari beberapa bagian, pada bagian pertama ini akan difokuskan pada pedoman umum sistem manajemen pengamanan data dan informasi.

Dengan ditetapkannya SPLN S5.008-1, maka segala ketentuan prihal *cyber security* harus mengikuti SPLN ini dan segala ketentuan sebelumnya yang bertentangan dengan standar ini dinyatakan tidak berlaku lagi.

Cyber Security Bagian 1: Pedoman Umum Sistem Manajemen Pengamanan Data dan Informasi

1 Ruang lingkup

Standar ini dimaksudkan sebagai pedoman dalam mengelola sistem pengamanan data dan informasi yang ada di lingkungan PLN. Manajemen pengamanan meliputi bagian *information technology* (IT) dan *operational technology* (OT).

2 Tujuan

Standar ini ditujukan untuk memberikan pedoman yang terarah dan seragam dalam pengelolaan dan pengaturan pengamanan data dan informasi di lingkungan PLN.

3 Acuan normatif

Ketentuan yang digunakan dalam SPLN ini mengikuti standar dan referensi berikut, kecuali ditetapkan secara khusus. Dalam hal terjadi revisi pada standar dan referensi tersebut, maka ketentuannya mengikuti edisi terakhirnya.

- a. ISO 27001, *Information Security Management Systems*
- b. ISO 27002, *Information security, cybersecurity and privacy protection*
- c. IEC 62351, *Cyber Security Series for the Smart Grid*
- d. IEC 62351-3, *Security for any profile including TCP IP;*
- e. IEC 62351-5, *Security for any profile including IEC 61850;*
- f. IEC 62443/ISA99, *Industrial communication networks;*
- g. IEC 60870-5, *Telecontrol equipment and systems;*
- h. IEC 61850, *Communication networks systems in substations;*
- i. Permen ESDM No. 20 Tahun 2020, Aturan Jaringan Sistem Tenaga Listrik (Grid Code)
- j. Perdir PLN Nomor 0061.P/DIR/2023, *Kebijakan Strategis Teknologi Informasi di Lingkungan PT PLN (persero);*
- k. SPLN S3.001: 2021 Peralatan SCADA Sistem Tenaga Listrik;
- l. SPLN S3.005-2:2021 Spesifikasi Peralatan Remote Station Bagian 1: Transmisi.

4 Istilah dan definisi

4.1

Applet

Sebuah program kecil yang berjalan di dalam konteks program lain, biasanya sebuah *browser web*. *Applet* sering digunakan untuk menyajikan konten interaktif atau fitur khusus pada halaman *web*. *Applet* ditulis dalam bahasa pemrograman seperti *Java*, dan untuk menjalankannya, *browser web* memerlukan *plugin* yang sesuai

4.2

Development environment

Lingkungan di mana perangkat lunak, aplikasi, atau sistem sedang dikembangkan dan diuji oleh pengembang. Ini adalah tahap awal dalam siklus pengembangan perangkat lunak, di mana kode ditulis, di-debug, dan diuji untuk memastikan bahwa fitur dan fungsi baru berfungsi dengan benar sebelum diteruskan ke tahap pengujian yang lebih ketat atau ke lingkungan produksi.

4.3

Information technology (IT)

Disebut juga teknologi informasi, adalah bidang yang mencakup penggunaan komputer, jaringan, perangkat keras, perangkat lunak, dan sistem elektronik lainnya untuk memproses, menyimpan, dan mengelola data serta informasi. Komponen utama meliputi: perangkat keras (*hardware*), perangkat lunak (*software*), jaringan (*networking*), dan data.

4.4

Mobile device PLN

Semua peralatan perangkat elektronik portabel yang dirancang untuk digunakan ketika bergerak atau dalam perjalanan yang dimiliki atau dikelola oleh PLN. *Mobile device* yang dimaksud meliputi semua perangkat elektronik yang digunakan untuk kegiatan bisnis dan operasional di lingkungan PLN.

4.5

Kriptografi

Ilmu dan seni tentang menyembunyikan dan melindungi informasi agar hanya dapat diakses atau dimengerti oleh pihak-pihak yang berwenang. Prinsip kriptografi meliputi enkripsi (pengacakan informasi), dekripsi (mengembalikan informasi yang dienkripsi) dan kunci (algoritma yang digunakan untuk mengacak/menyembunyikan informasi).

4.6

Manajemen PLN

Manajemen PLN adalah pemimpin organisasi dapat berupa direksi PLN, kepala divisi, dan pemimpin unit. Manajemen PLN dapat juga menunjuk orang/bidang/posisi

jabatan/kelompok yang ditunjuk oleh yang tersebut sebelumnya dalam bertanggung jawab untuk mengelola fungsi tertentu sebagai representasi manajemen PLN.

4.7

Operation technology (OT)

Disebut juga teknologi operasi, teknologi perangkat keras dan perangkat lunak yang mendeteksi atau menyebabkan perubahan melalui pemantauan dan pengendalian perangkat, proses, dan kejadian fisik di perusahaan. Komponen utama meliputi: perangkat keras (*hardware*) yang dapat meliputi *Programmable Logic Controllers (PLC)*, *Distributed Control Systems (DCS)*, *Supervisory Control and Data Acquisition (SCADA)*, dan Sensor dan Aktuator dan perangkat lunak (*software*) seperti *Human-Machine Interface (HMI)* dan Sistem Manajemen Produksi/*Manufacture Execution System (MES)*.

4.8

Pekerja

Pegawai atau non-pegawai PLN yang melakukan pekerjaan di lingkungan PLN.

4.9

Production environment (lingkungan kerja)

lingkungan di mana perangkat lunak, aplikasi, atau sistem berjalan dan digunakan oleh pengguna akhir. Ini adalah tahap akhir dalam siklus pengembangan perangkat lunak, di mana aplikasi telah melalui pengujian dan verifikasi yang ketat dan siap untuk digunakan dalam operasi sehari-hari

4.10

Protokol

Sekumpulan semantik dan aturan cara penulisan (sintaksis) yang menentukan cara unit fungsional dalam berkomunikasi. [ISO/IEC 2382-9].

4.11

Sistem produksi

Semua peralatan dan aplikasi operasional yang sudah berjalan.

4.12

Secure area

Secure area atau zona pengamanan adalah ingkungan atau zona yang diatur sedemikian rupa untuk memberikan tingkat keamanan yang tinggi terhadap akses yang tidak sah atau serangan siber

4.13

Staging environment (lingkungan uji coba)

Lingkungan pengujian yang meniru lingkungan produksi secara erat untuk memastikan bahwa perangkat lunak atau aplikasi berfungsi dengan benar sebelum diterapkan ke produksi. Lingkungan ini digunakan sebagai tempat pengujian akhir untuk mendeteksi masalah yang mungkin tidak terdeteksi di lingkungan pengembangan.

5 Fungsi dan peran organisasi keamanan data dan informasi

5.1 Peran dan tanggung jawab keamanan data dan informasi

Berikut peranan dan tanggung jawab keamanan data dan informasi:

a. Manajemen PLN

Manajemen PLN bertanggung jawab atas tata kelola PLN secara keseluruhan atas organisasi yang dipimpinnya, termasuk di dalamnya manajemen dan kontrol risiko keamanan data dan informasi.

Manajemen PLN perlu memberikan arahan strategis secara menyeluruh dengan menyetujui dan memberikan wewenang atas pelaksanaan kebijakan ini, dan mendeklasifikasi tanggung jawab operasional atas keamanan fisik dan keamanan data dan informasi kepada organisasi yang ditunjuk.

Manajemen PLN memberikan kewenangan kepada organisasi yang ditunjuk untuk bertanggung jawab terhadap tata kelola untuk mengoordinasikan dan memastikan pembuatan dokumen pendukung dari kebijakan ini.

Pimpinan unit kerja di PLN bertanggung jawab untuk:

1. Mengimplementasikan kebijakan ini beserta dokumen pendukungnya dalam pekerjaan sehari-hari.
2. Memastikan bahwa kontrol teknik, fisik, dan prosedural yang tepat diaplikasikan dan digunakan oleh seluruh pekerja.
3. Setiap pimpinan unit kerja harus memastikan bahwa:
 - Seluruh pekerja diberikan informasi mengenai kewajiban pekerja untuk memenuhi kebijakan perusahaan melalui kegiatan awareness, pelatihan, dan edukasi.
 - Patuh pada kebijakan dan secara aktif mendukung kontrol tersebut di atas.
 - Dipantau untuk dinilai seberapa jauh kepatuhan pekerja terhadap kebijakan dan diingatkan kembali akan kewajiban yang harus mereka takukan.
 - Memberikan arahan, dukungan sumber daya, dan review untuk memastikan aset data dan informasi diproteksi secara tepat dalam lingkup tanggung jawab mereka.

- Menginformasikan *information security manager* (ISM) dan/atau *information owner* mengenai kejadian aktual atau kejadian yang ditengarai melanggar kebijakan (insiden keamanan data dan informasi) yang berdampak pada aset di bawah tanggung jawab mereka.
 - Mengevaluasi kepatuhan terhadap prinsip kebijakan secara berkala melalui audit internal.
- b. Peran dan tanggung jawab *information security manager* (ISM)
- ISM adalah personel yang bertanggung jawab penuh dalam pengembangan dan implementasi keamanan data dan informasi. ISM harus ditunjuk oleh manajemen PLN dan bertanggung jawab untuk:
1. Menjabarkan kebijakan dan prosedur keamanan data dan informasi secara teknis dan non-teknis.
 2. Mendukung pemilik informasi atau *information owner* dan manajer dalam mendefinisikan dan mengimplementasikan kontrol agar sesuai dengan kebijakan dan mengelola risiko keamanan data dan informasi.
 3. Memahami dan mengantisipasi eksposur risiko sistem informasi, serta mengembangkan langkah penanganan yang tepat dan memadai
 4. Mengusulkan inisiatif utama dalam meningkatkan keamanan data dan informasi PLN
 5. Mengelola anggaran program dan proyek untuk menjamin efektivitas biaya untuk manajemen sistem keamanan data dan informasi
 6. Mengkaji dan memantau kepatuhan terhadap kebijakan, dan memberikan input kepada audit internal.
 7. Mengumpulkan, menganalisis, dan memberikan komentar terhadap laporan dan insiden keamanan data dan informasi.
 8. Mendukung *information owner* dalam investigasi dan pemulihan insiden keamanan data dan informasi atau pelanggaran lain terhadap kebijakan.
 9. Bekerjasama dengan berbagai unit kerja internal terkait seperti manajemen risiko, hukum dan kepatuhan, audit internal, dan pihak-pihak eksternal seperti kepolisian bila diperlukan.
 10. Mengkoordinasikan kesadaran keamanan data dan informasi dalam menumbuhkan budaya keamanan dan kepatuhan kepada kebijakan keamanan data dan informasi.
- c. Peran dan tanggung jawab *information owner*

Information owner adalah atasan yang berwenang yang diberikan tanggung jawab oleh Manajemen PLN untuk melindungi aset data dan informasi. *Information owner* dapat mendelegasikan tugas keamanan data dan informasi kepada atasan yang berwenang atau individu lain namun tetap *accountable* atas implementasi tugas tersebut. *Information owner* bertanggung jawab untuk:

1. Melakukan klasifikasi dan proteksi yang tepat atas aset data dan informasi sesuai dengan klasifikasi informasi yang berlaku di PLN.
 2. Menentukan dan membiayai kontrol yang sesuai.
 3. Memberikan akses ke aset data dan informasi sesuai dengan klasifikasi dan kebutuhan bisnis.
 4. Mengawasi pengkajian risiko keamanan data dan informasi untuk memastikan persyaratan keamanan data dan informasi ditetapkan secara jelas dan tepat dan didokumentasikan sejak tahap awal pengembangan.
 5. Memastikan *review* berkala terhadap akses sistem/data.
 6. Memantau kepatuhan terhadap kebijakan perlindungan aset yang berada di bawah tanggung jawab mereka.
- d. Peran dan tanggung jawab *user*

User adalah seluruh pengguna sumber daya komputer, aset data dan informasi, serta fasilitas pemrosesan data dan informasi yang bertanggung jawab dalam keamanan seluruh fasilitas pemrosesan data, informasi, perangkat, serta aset yang terasosiasi dengan data dan informasi tersebut.

5.2 Pemisahan wewenang

Beberapa hal yang diperhatikan terkait pemisahan wewenang:

- a. Pemisahan tanggung jawab pekerjaan

Tanggung jawab pekerjaan dan area harus dipisahkan untuk mengurangi kemungkinan perubahan atau penyalahgunaan oleh pihak yang tidak berwenang. Lebih lanjut, pemisahan tugas dan tanggung jawab masing-masing individu harus diatur secara jelas untuk:

1. Mengurangi kesempatan akses bagi yang tidak berhak.
2. Mengurangi kemungkinan perubahan yang tidak diotorisasi/disengaja
3. Mengurangi penyalahgunaan data dan informasi atau aset data dan informasi oleh pihak yang tidak berwenang

- b. Pemisahan tugas

Dalam melakukan aktivitas operasional harus diterapkan pemisahan tugas dan tanggung jawab antara pelaksana dan pemberi otorisasi.

- c. Pemantauan fungsi administrator

Untuk mencegah penyalahgunaan, pekerja yang mendapat hak akses sebagai admin atau *super user* harus dipantau secara khusus oleh personel lain. Fungsi pemantauan harus dilakukan secara independen.

d. Kontrol tambahan atas risiko penyalahgunaan wewenang

Jika terdapat risiko penyalahgunaan wewenang atau kontrol tidak berjalan secara efektif, maka kontrol tambahan harus dibuat dan diterapkan misalnya dengan *pelaksanaan audit internal* yang direview secara rutin.

1. Hubungan dan kontak dengan pihak berwenang

Perlu dibangun dan dijaga hubungan baik dan kontak dengan pihak-pihak yang berwenang, regulator, otoritas penegak hukum, lembaga kepemerintahan, penyedia layanan informasi, dan operator telekomunikasi untuk memastikan bahwa tindakan yang tepat diambil apabila terjadi insiden keamanan. Pelaporan insiden keamanan data dan informasi kepada pihak berwenang apabila terdapat pelanggaran atas peraturan, hukum atau perundang-undangan harus menjadi bagian dari proses manajemen insiden keamanan.

2. Keamanan data dan informasi dalam manajemen proyek

Keamanan data dan informasi adalah bagian yang tidak terpisahkan dalam manajemen proyek. Manajer proyek bertanggung jawab untuk memastikan keamanan yang mencakup *confidentiality*, *integrity*, dan *availability* terhadap dokumentasi dan *deliverable* proyek, dengan mempertimbangkan antara lain:

- Pembuatan *project charter* yang terstandardisasi.
- Identifikasi *stakeholder* untuk mengelola konflik kepentingan.
- Metode komunikasi aktif melalui media yang aman.
- Persyaratan keamanan untuk tim proyek.
- Manajemen risiko perihal keamanan.
- Manajemen otentikasi dan akses.
- Kebutuhan enkripsi.

6 **Mobile device dan teleworking**

6.1 **Kebijakan mobile device**

Kebijakan formal dan langkah-langkah keamanan harus ditetapkan untuk melindungi penggunaan *mobile device*, antara lain:

- a. Kontrol keamanan yang sesuai harus digunakan saat menggunakan fasilitas *mobile device* seperti laptop (*notebook*) dan *smartphone* yang digunakan untuk mengakses atau menyimpan data PLN.
- b. Kontrol akses fisik yang tepat harus digunakan untuk melindungi peralatan *mobile device*, serta tidak boleh ditinggalkan tanpa pengawasan yang terkendali (contoh: di mobil, hotel/ ruang konferensi, ruang publik terbuka). Selain itu, kontrol akses *logic* (contoh: otentikasi user dan enkripsi data yang tersimpan) juga harus digunakan.

- c. Seluruh pengguna peralatan *mobile device* harus diberikan petunjuk pengamanan *mobile device*.
- d. Peralatan *mobile device* yang disediakan oleh PLN untuk pegawai dan mitra kerja tidak diperkenankan digunakan untuk urusan pribadi yang bertentangan dengan kepentingan perusahaan.
- e. Pengguna *mobile device* bertanggung jawab untuk melakukan *backup* data secara rutin dan melindungi semua media *backup* dari pencurian, kehilangan, atau kerusakan.
- f. Sistem operasi dan aplikasi pada *mobile device* perlu dipelihara, termasuk pemasangan *patching*, *personal firewall*, dan perlindungan dari virus dan *malware*. Pengguna tidak diperkenankan mengubah keamanan teknis tersebut dengan cara mematikan atau melakukan konfigurasi ulang.
- g. Hanya *mobile device* PLN yang boleh terhubung ke jaringan atau sistem informasi PLN. Peralatan *mobile device* PLN hanya boleh digunakan oleh pegawai atau mitra kerja yang bekerja di bawah perjanjian dengan PLN, untuk tujuan bisnis PLN.
- h. Peralatan *mobile device* milik mitra kerja hanya boleh terhubung ke jaringan atau sistem PLN saat sedang digunakan untuk pekerjaan PLN sesuai dengan perjanjian kerjasama.
- i. Semua peralatan *mobile device* yang dimiliki PLN atau yang diizinkan berada dalam jaringan PLN harus dapat teridentifikasi (misalnya melalui *MAC Address*) dan penggunaanya dapat diasosiasikan dengan personel tertentu, sebelum terhubung ke jaringan PLN.
- j. Personel yang menggunakan peralatan *mobile device* PLN di area publik harus memastikan keamanan data dan informasi terkait otentikasi ataupun informasi sensitif lainnya.

6.2 Kebijakan *teleworking*

Rencana operasional, kebijakan dan prosedur harus ditetapkan dan diimplementasikan untuk aktivitas *teleworking*, antara lain:

- a. *Teleworking* (bekerja di luar kantor dan terkoneksi dengan jaringan PLN secara *remote*) hanya diizinkan apabila memiliki hak akses yang sah dengan alokasi dan keperluan yang jelas.
- b. *Teleworker* harus mempertimbangkan keamanan fisik lokasi *teleworking* termasuk lokasi dan lingkungan setempat. Peralatan yang digunakan *teleworker*, media penyimpanan, dan kertas kerja harus dilindungi dari campur tangan anggota keluarga, rekan kerja, dan pihak yang tidak berkepentingan.
- c. *Teleworker* harus melindungi peralatan, data, dan semua bagian lain dari infrastruktur PLN dari kerusakan sebagai akibat dari aktivitas pekerjaan. Pengguna bertanggung jawab untuk melindungi peralatan dari akses tidak sah, pencurian, kerusakan, atau kehilangan.

- d. Sebelum menggunakan peralatan *teleworking*, *teleworker* harus diberi pemahaman tentang pengamanan fasilitas *teleworking* dan harus menandatangani pernyataan memahami dan mematuhi kebijakan pengamanan data dan informasi.
- e. Akses *remote*, sistem jaringan, dan data PLN harus dikontrol dengan perangkat keamanan (seperti: *firewall*, anti virus, dll) dan mekanisme pengamanan lain.
- f. Akses *teleworking* menggunakan lalu lintas jaringan yang aman.
- g. Atasan yang terkait bertanggung jawab mengawasi *teleworker* untuk memastikan *teleworker* mematuhi kebijakan keamanan dan persyaratan bisnis terkait.

7 Keamanan sumber daya manusia

7.1 Sebelum masa kerja

7.1.1 Pemeriksaan latar belakang

Seluruh personel yang potensial untuk direkrut harus diseleksi sebelum dipekerjakan, khususnya untuk posisi sensitif atau penting yang membutuhkan tanggung jawab besar dimana integritas (kejujuran dan keterpercayaan) dan kompetensi (keahlian, pengalaman, dan kualifikasi). Proses seleksi dimaksudkan untuk mengurangi risiko mempekerjakan orang yang tidak tepat. Verifikasi harus dilakukan untuk melakukan konfirmasi atas kelengkapan dan akurasi data calon personel yang potensial untuk direkrut.

7.1.2 Syarat dan ketentuan pekerjaan

Beberapa hal yang diperhatikan terkait syarat dan ketentuan pekerjaan.

a. Aturan pelaksanaan perusahaan

Semua pegawai harus membaca, memahami dan berperilaku sesuai dengan aturan pelaksanaan perusahaan.

b. Perjanjian kerahasiaan/*non-disclosure agreement* (NDA) internal PLN

Sebagai bagian dari perjanjian kontrak kerja antar unit atau antara organisasi dengan personal, pihak yang terkait harus:

1. Menyetujui dan menandatangani pernyataan kerahasiaan sesuai kontrak perjanjian.
2. Melaksanakan pernyataan kerahasiaan sesuai kontrak perjanjian.

c. Perjanjian kerahasiaan/*non-disclosure agreement* (NDA) dengan eksternal PLN

Sebagai bagian dari perjanjian kerja sama antara PLN dengan lembaga eksternal, pihak yang terkait harus menandatangani perjanjian/pernyataan kerahasiaan yang membatasi pengungkapan segala sesuatu yang berkenaan dengan kerahasiaan PLN ke pihak lain.

d. Hak kekayaan intelektual

Seluruh pegawai harus memberikan hak eksklusif untuk hak paten, hak cipta, penemuan atau hak intelektual lainnya yang ditemukan atau dikembangkan kepada PLN.

e. Tanggung jawab keamanan data dan informasi

Seluruh pegawai harus memahami dan mematuhi seluruh ketentuan keamanan data dan informasi yang berlaku, mencakup kebijakan, prosedur, dan peraturan lainnya.

7.2 Selama masa kerja

7.2.1 Tanggung jawab manajemen PLN

Tanggung jawab pengamanan informasi harus ditetapkan dalam deskripsi pekerjaan seluruh pegawai jika terdapat kebutuhan untuk mengakses informasi sensitif, berharga, atau kritis. Manajemen perlu memastikan bahwa setiap pegawai PLN maupun mitra kerja yang mengakses informasi atau fasilitas pemrosesan informasi untuk diberikan:

- a. Pengarahan akan kesadaran atas tanggung jawab pekerja terhadap keamanan data dan informasi sebelum diberikan akses ke jaringan, sistem, atau data PLN secara berkala.
- b. Arahan untuk memenuhi tanggung jawab pekerja yang berkaitan dengan pengamanan informasi melalui supervisi dan dukungan secara berkesinambungan.
- c. Kompetensi, kemampuan, dan kualifikasi pekerja mengenai keamanan data dan informasi melalui kegiatan *security awareness*, edukasi, dan pembinaan.

7.2.2 Evaluasi Kinerja

Kepatuhan atas kebijakan-kebijakan dan prosedur-prosedur pengamanan informasi harus menjadi pertimbangan dalam semua evaluasi kinerja pegawai.

7.2.3 Kesadaran, edukasi, dan pelatihan keamanan data dan informasi

Selama masa kerja pekerja harus diberikan kesadaran, edukasi dan pelatihan keamanan data dan informasi dengan ketentuan sebagai berikut.

a. Pelatihan keamanan data dan informasi

Semua pekerja harus mendapatkan edukasi yang tepat dan terkini secara berkala mengenai kebijakan dan prosedur keamanan data dan informasi yang terkait dengan fungsi kerja masing-masing, termasuk diberikan pelatihan dan bahan referensi penunjang yang cukup yang memungkinkan mereka dalam melindungi sumber daya informasi milik PLN.

b. Pembinaan keamanan data dan informasi

Kegiatan *security awareness*, edukasi, dan pembinaan harus merefleksikan kebutuhan pekerja, sebagai contoh:

1. Pimpinan perusahaan atau pimpinan unit kerja harus memahami tugas dan tanggung jawabnya dalam pengelolaan keamanan data dan informasi.
2. Pekerja harus memahami aspek-aspek teknis dari pengamanan data dan informasi.
3. Pekerja harus diingatkan secara berkala mengenai kewajibannya untuk menjaga kerahasiaan aset data dan informasi dan integritas pekerja.

c. Tanggung jawab keamanan data dan informasi

Tanggung jawab terhadap keamanan data dan informasi keseharian adalah tugas setiap pegawai.

7.2.4 Tindakan kedisiplinan

Tindak kedisiplinan meliputi:

a. Konsekuensi dari ketidakpatuhan

Ketidakpatuhan dengan kebijakan, standar, atau prosedur pengamanan informasi dapat menjadi dasar untuk melakukan tindakan pendisiplinan bahkan sampai dengan pemberhentian.

b. Konsekuensi dari pelanggaran

Dengan mengasumsikan suatu pelanggaran sebagai: kelalaian, tanpa sengaja atau kebetulan, maka tindak lanjut pelanggaran tersebut dapat ditindaklanjuti sesuai dengan peraturan internal PLN.

c. Pemberhentian hubungan kerja

Pihak yang melakukan pencurian properti milik PLN, melakukan pembangkangan, atau terlibat kejahatan pidana harus segera diakhiri hubungan kerjanya, selanjutnya dilakukan pendampingan saat pengumpulan dan pemindahan barang-barang pribadinya dan dikawal keluar dari area PLN.

d. Pemberhentian secara paksa

Perangkat pribadi yang digunakan oleh pekerja untuk mengakses data dan informasi yang diberhentikan secara paksa, harus segera diisolasi dari internet dan jaringan internal PLN, dijaga keutuhan data dan fisik, serta diinvestigasi lebih lanjut untuk kebutuhan forensik jika dibutuhkan.

7.3 Pemutusan dan perubahan kerja

7.3.1 Tanggung jawab pemutusan dan perubahan kerja

Berikut beberapa hal yang diperhatikan terkait tanggung jawab pemutusan dan perubahan kerja meliputi:

a. Proses pemutusan hubungan kerja

Pimpinan unit kerja bertanggung jawab untuk memastikan bahwa proses pemutusan hubungan kerja telah dilakukan sebelum pekerja secara resmi meninggalkan PLN. Pekerja harus diingatkan mengenai tanggung jawab secara hukum dan etika untuk menjaga kerahasiaan informasi yang didapat selama masa kerjanya.

b. Pengembalian aset dalam pemutusan kerja

Seluruh pegawai dan mitra kerja harus mengembalikan seluruh aset milik PLN jika terjadi proses pemutusan hubungan kerja, kontrak atau perjanjian.

c. Penghapusan hak akses dalam pemutusan kerja

Hak akses user seluruh pegawai dan mitra kerja pada fasilitas pengolahan informasi PLN harus dihapus setelah proses pemutusan hubungan kerja, penghentian kontrak atau perjanjian, atau disesuaikan apabila terdapat pergantian.

8 Manajemen aset

Pengelolaan aset mengacu pada prosedur atau aturan yang berlaku di PLN.

8.1 Tanggung jawab untuk aset

8.1.1 Pengadaan aset

Proses pengadaan aset harus melalui persetujuan dan prosedur yang berlaku dengan mempertimbangkan kebutuhan pengguna, biaya, kualitas, serta kebutuhan pengamanan data dan informasi pada aset. Setelah diterima, aset harus diperiksa untuk memastikan kesesuaian dengan spesifikasi.

8.1.2 Inventaris aset

Tanggung jawab inventarisasi aset yang perlu dilakukan oleh manajemen antara lain:

- a. Manajemen harus mengidentifikasi semua aset data dan informasi PLN dan mengklasifikasikannya, sehingga dapat diterapkan pengamanan yang tepat dan sesuai.
- b. Manajemen harus menjaga inventarisasi semua aset data dan informasi yang telah diidentifikasi selalu lengkap dan akurat, termasuk informasi klasifikasi, lokasi, sistem operasi, versi dan sebagainya.

- c. PLN harus memastikan perlindungan aset data dan informasi yang efektif dengan menciptakan dan mengelola inventarisasi aset data dan informasi terkini secara terus-menerus.

8.1.3 Klasifikasi dan pelabelan/identifikasi aset

Aset data dan informasi harus dikategorikan sesuai dengan kepentingan unit bisnis dalam organisasi dan tingkat keamanannya, serta diberikan label/identifikasi sesuai dengan ketentuan yang berlaku.

8.1.4 Kepemilikan aset

Kepemilikan aset data dan informasi dikelola sebagai berikut:

- a. Pemilik aset (*asset owner*) akan menyimpan, memelihara dan memperbarui *database* dari semua data dan aset yang dimiliki.
- b. *Information owner* bertanggung jawab untuk mengamankan seluruh aset data dan informasi dibawah tanggung jawabnya, serta menentukan pembatasan akses dan kontrol keamanan lainnya terhadap aset data dan informasi.
- c. Semua aset data dan informasi yang dimaksud berupa semua aset fisik ataupun digital (contoh: lisensi, *software*, dll).

8.1.5 Acceptable use of asset

Acceptable use dari aset perlu didefinisikan untuk menjelaskan hal yang diizinkan dan tidak diizinkan/dilarang dalam penggunaan aset terkait informasi. Pekerja harus mengikuti ketentuan *acceptable use* yang telah didefinisikan pada saat menggunakan aset untuk operasional bisnis.

8.1.6 Pengelolaan dan pemeliharaan aset

Aset harus dikelola, dipantau, dan dipelihara untuk memastikan aset dapat berfungsi dan/ atau digunakan dengan baik. Pemeliharaan aset dilakukan secara berkala sesuai ketentuan dan/atau sesuai periode yang disarankan oleh pabrik (*manufacturers specification*). Selama masa pemeliharaan, PLN harus memastikan keamanan data dan informasi yang ada pada aset tetap terjaga. Pengaturan atau modifikasi terhadap konfigurasi aset harus dilakukan dengan persetujuan pemilik aset.

8.1.7 Pengembalian aset

Seluruh pegawai dan mitra kerja harus mengembalikan seluruh aset milik PLN jika terjadi proses pemutusan hubungan kerja, kontrak atau perjanjian. Aset yang dikembalikan perlu diperiksa dan diverifikasi kembali untuk mendeteksi adanya kecacatan, gangguan, atau kerusakan yang ada pada aset.

8.1.8 Penghapusan aset

Setiap aset data dan informasi yang dihapus harus melalui prosedur penghapusan dengan mempertimbangkan agar keamanan data dan informasi tetap terjaga.

8.2 Klasifikasi informasi

Berikut beberapa ketentuan terkait dengan klasifikasi informasi.

a. Tingkatan klasifikasi informasi

Data, informasi, terutama yang berkenaan dengan bisnis PLN harus dikategorikan sesuai dengan kepentingan unit bisnis organisasi dan tingkat keamanannya. Klasifikasi informasi berlaku untuk semua aset data dan informasi PLN.

1. *Public.* Informasi yang dapat diakses oleh siapa pun, baik di dalam maupun di luar organisasi. Informasi ini biasanya tidak mengandung data sensitif atau rahasia. Aset data dan informasi yang secara sengaja disediakan oleh PLN untuk diketahui oleh seluruh stakeholder/masyarakat umum.

Contoh: laporan keuangan perusahaan yang sudah rilis, tarif dasar listrik yang sudah disahkan, dan alamat kantor.

2. *Internal.* Informasi yang hanya dapat diakses oleh anggota internal suatu organisasi. Informasi ini mungkin mengandung rincian operasional atau data yang hanya relevan untuk anggota organisasi tersebut. Aset data dan informasi yang dimiliki oleh PLN yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan mengganggu citra dan reputasi PLN.

Contoh: informasi perusahaan, rekanan, dan beberapa data pribadi, atau data lain yang ditetapkan sebagai data rahasia (*confidential*) dibawah kesepakatan rekanan, tapi tidak diatur dalam peraturan.

3. *Restricted.* Informasi yang memiliki tingkat kerahasiaan lebih tinggi daripada informasi internal. Informasi ini hanya dapat diakses oleh sejumlah terbatas orang yang memiliki izin khusus. Aset data dan informasi PLN yang apabila didistribusikan tidak sah atau jatuh ke tangan orang lain akan mengganggu kelancaran kegiatan bisnis perusahaan dan merusak citra perusahaan.

Contoh: Data yang berisikan kegiatan bisnis yang ditujukan pada kelompok pegawai tertentu, dokumen persetujuan kontraktor yang hanya sebatas informasi general, Data personal, *client* dan internal, atau dokumen rahasia lain yang ditetapkan dalam kategori *restricted*.

4. *Confidential*. Informasi yang sangat sensitif dan rahasia, dan biasanya hanya dapat diakses oleh pihak yang sangat terbatas dan memiliki izin khusus. Pelanggaran kerahasiaan informasi ini dapat memiliki konsekuensi hukum serius. Aset data dan informasi PLN yang sangat sensitif, dan bersifat strategis yang apabila didistribusikan secara tidak sah atau jatuh ke tangan orang yang tidak berhak akan menyebabkan kerugian keuangan atau kehancuran bisnis bagi perusahaan dan/atau mengganggu sistem kelistrikan nasional.

Contoh: Data obligasi perusahaan, data keuangan internal, dokumen struktur gedung *data center*, atau aset data dan informasi lain yang ditetapkan dalam kategori *confidential*.

5. *Personal* - Data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.

Contoh: nama, alamat, nomor telepon, dll.

b. Pelabelan informasi

Pelabelan informasi harus diterapkan secara konsisten mengikuti tingkatan klasifikasi informasi, seperti pada dokumen *softcopy* dan *hardcopy*, media elektronik, dan lainnya. Informasi yang diterima dari pihak ketiga dapat diberikan klasifikasi ketika diterima oleh PLN, atau diklasifikasikan kembali menurut level klasifikasi PLN.

c. Penanganan aset

Kumpulan prosedur yang sesuai untuk penanganan aset data dan informasi harus dikembangkan dan diimplementasikan berdasarkan klasifikasi yang telah ditentukan.

d. Klasifikasi sistem dan perangkat lunak

Sistem dan perangkat lunak terutama yang berkenaan dengan bisnis PLN harus dikategorikan sesuai dengan kepentingan bisnis dan tingkat pengamanannya.

8.3 Penanganan media penyimpanan data dan informasi

Beberapa ketentuan terkait media penyimpanan data dan informasi:

a. Manajemen *removable media*

Prosedur untuk penanganan, penyimpanan, dan pengamanan *removable media* harus minimal mempertimbangkan poin sebagai berikut:

1. Pengamanan fisik yang memadai untuk media yang menyimpan data/informasi sensitif atau rahasia.
2. Penggunaan media baru dengan pengamanan sesuai klasifikasi data/informasi untuk pendistribusian kepada pihak diluar PLN.
3. Data/informasi yang disimpan sesuai dengan kebutuhan bisnis. Apabila tidak dibutuhkan, agar segera dihapus.

4. Data/informasi yang disimpan dalam *removable media* agar diperiksa secara berkala dan dipindahkan ke media baru untuk menghindari penurunan kualitas dan/atau kehilangan data.
 5. Media harus dipelihara untuk mencegah adanya kerusakan atau gangguan pada media, seperti *bad sector*, virus.
 6. *Removable media* perlu dilindungi dengan mempertimbangkan klasifikasi keamanan data dan informasi (contoh: enkripsi dan pengamanan fisik).
- b. Penanganan informasi
- Prosedur keamanan untuk menangani dan menyimpan informasi penting harus dibuat dalam rangka melindungi informasi dari penyalahgunaan, sesuai dengan klasifikasi informasi.
- c. Pemusnahan data dan informasi
- Perangkat atau media pengolah informasi atau penyimpan data yang sudah tidak digunakan lagi harus disanitasi sesuai dengan prosedur keamanan yang telah ditetapkan, untuk memastikan data/informasi yang ada di dalam media tidak dapat dikembalikan.
- d. Pemindahan media fisik

Pada saat pemindahan, media harus terlindungi dari potensi akses yang tidak sah, seperti kerusakan, pencurian, intersepsi, dan duplikasi media. Berikut adalah yang perlu dipertimbangkan pada saat transfer media:

1. Penggunaan jasa kurir yang telah mengirim media merupakan *supplier* yang terpercaya.
2. Perlindungan media dari kerusakan fisik atau gangguan lingkungan lainnya, dengan mempertimbangkan spesifikasi pabrik misalnya kerentanan dari suhu, kelembaban, dan medan magnet.
3. Pencatatan atas aktivitas transportasi media perlu dilakukan, pada saat dilakukan pengiriman sampai media telah diterima sesuai tujuan

9 Kontrol akses

9.1 Kebutuhan bisnis atas kontrol akses

9.1.1 Kebijakan kontrol akses

Standar kontrol akses sumber daya data dan informasi yang ditetapkan harus dapat mencegah akses yang tidak sah terutama terkait dengan pemenuhan kebutuhan bisnis. Kebijakan dan standar akan dikaji ulang secara terus menerus untuk memastikan kesesuaian tetap terjaga, dengan memperhatikan:

- a. Persyaratan keamanan data dan informasi untuk aplikasi bisnis masing-masing.

- b. Prinsip-prinsip keamanan data dan informasi yang fundamental, seperti *default deny* dan konsep *least privileged* atau pemberian hak akses minimum.
- c. Identifikasi dan klasifikasi asset data dan informasi yang terkait.
- d. Hukum dan perjanjian kerjasama mengenai perlindungan akses data atau layanan.
- e. Pemisahan tugas (misalnya permohonan dan otorisasi dilakukan oleh personel yang berbeda).

Akses ke informasi milik PLN, atau yang berada di bawah kontrol PLN harus diberikan berdasarkan kebutuhan. Informasi diungkapkan hanya kepada orang-orang yang memiliki kebutuhan bisnis dan hak akses yang sah untuk informasi dengan mempertimbangkan prinsip – prinsip antara lain:

- a. Prinsip *least privilege*

Pemberian akses harus mengikuti prinsip *least privilege*, yaitu pemberian hak akses minimum sesuai dengan kebutuhan.

- b. Prinsip *deny default access*

Semua akses terhadap PLN informasi, data, *file*, jaringan dan sistem secara *default* adalah ditolak (*deny*), kecuali secara eksplisit diijinkan.

- c. Prinsip pemisahan akses

Pemberian akses harus mempertimbangkan pemisahan akses (*segregation of duties*) untuk menghindari penyalahgunaan akses.

- d. Prinsip keamanan independen

Semua sistem informasi dan pengamanannya tidak boleh dibatasi oleh keadaan/keterbatasan perangkat keras/ lunak atau oleh layanan yang disediakan oleh pihak ketiga.

- e. Menghapus dan/atau menonaktifkan *default user*

Seluruh *default* akses seperti user *default* sistem operasi, bawaan mitra kerja, bawaan perangkat keras/lunak harus diganti, dihapus atau dinonaktifkan untuk mengurangi risiko penyalahgunaan.

- f. Pemberitahuan modifikasi tingkat akses

Seluruh perubahan akses kontrol harus memberikan pemberitahuan kepada pihak-pihak yang berkepentingan

- g. Pemantauan akses dan penggunaan sistem

Akses ke seluruh sumber daya data dan informasi milik PLN harus selalu dicatat dan dipantau untuk mengidentifikasi potensi penyalahgunaan sistem atau informasi.

h. Tingkat dan klasifikasi keamanan

Manajemen menetapkan tingkat perlindungan dan keamanan yang berbeda untuk setiap aset data dan informasi dan sistem pendukungnya sesuai dengan kepentingan bisnis dan klasifikasinya.

i. Peraturan dan kontrak yang relevan

Penerapan kontrol akses harus memperhatikan dan mematuhi semua peraturan yang berlaku dan mematuhi perjanjian atau kontrak yang mengatur kegiatan bisnis organisasi.

j. Standar profil akses *user*

Semua sistem harus memiliki profil *user* dengan standar kriteria yang telah ditetapkan agar dapat membedakan jenis akses.

9.1.2 Akses ke jaringan dan layanan jaringan

Layanan jaringan harus dibatasi dan dilindungi dengan menerapkan prinsip *default deny*, yaitu secara *default* ditutup dan hanya dibuka didasarkan pada kebutuhan bisnis dengan memperhatikan aspek keamanan data dan informasi.

9.1.3 Kebijakan penggunaan layanan jaringan

Penerapan kebijakan penggunaan layanan jaringan harus mempertimbangkan hal sebagai berikut:

a. Pemutusan layanan

Manajemen PLN memiliki hak dan wewenang untuk memblokir, menyembunyikan, menolak dan menghentikan layanan tanpa pemberitahuan terlebih dahulu.

b. Kontrol akses jaringan

Kontrol pengamanan fisik dan *logic* harus diterapkan dalam membatasi akses tidak sah ke jaringan, *node* (contoh: *router*, *firewall*, server aplikasi, *workstation*) dan layanan jaringan (seperti *http/web*, layanan *e-mail*).

c. Persetujuan koneksi intranet dan internet

Pekerja tidak diperkenankan membuat sambungan jaringan eksternal untuk mendapatkan akses ke sistem data dan informasi PLN, kecuali setelah mendapatkan persetujuan dari Manajemen PLN. PLN juga harus memastikan:

1. Interkoneksi antara PLN dan jaringan pihak ketiga harus disetujui oleh Manajemen PLN dan kontrol akses jaringan interkoneksi harus dibuat, diimplementasikan, dan diawasi.
2. Semua koneksi internet ke peralatan/perangkat PLN harus mendapatkan persetujuan dari Manajemen PLN.

3. Akses pekerja ke layanan berbasis internet harus dicatat dan dibatasi hanya untuk tujuan bisnis.
- d. Memantau keamanan akses jaringan

Keamanan jaringan harus diawasi secara rutin dan segala risiko yang dapat muncul perlu dikaji dan dibuatkan skala prioritas. Kerentanan sistem yang kritis perlu diperbaiki dengan segera apabila terdapat ancaman yang signifikan. Apabila perbaikan tidak dapat dilakukan, kontrol alternatif harus diterapkan dalam memitigasi risiko.

- e. Parameter konfigurasi keamanan jaringan

Parameter konfigurasi keamanan jaringan (contoh: *rule firewall*, protokol, *port*) perlu didokumentasikan dan dikelola dengan kontrol perubahan, dan ditinjau berkala dalam memastikan ketepatan dan kesesuaianya.

- f. *Website* non bisnis

Sistem keamanan PLN dapat mendeteksi dan mencegah pengguna yang terhubung ke berbagai situs *web* non-bisnis.

- g. Kekayaan intelektual

Ketika mengakses internet menggunakan sistem PLN, pegawai dapat menggunakan materi yang diperoleh di internet setelah mendapatkan izin dari sumber, memberi tanda kutip pada materi dari sumber lain, dan mengungkapkan informasi internal perusahaan melalui internet hanya jika informasi tersebut secara resmi disetujui untuk disebarluaskan ke publik.

9.2 Manajemen akses *user*

Hal-hal yang perlu diperhatikan dalam manajemen akses *user* sebagai berikut.

- a. Registrasi dan penghapusan *user*

Semua akses terhadap sumber daya informasi PLN harus dilakukan melalui proses manajemen akses yang terdokumentasi, termasuk pembuatan akses *user*, perubahan akses *user*, dan penonaktifan atau penghapusan akses *user*, dengan mempertimbangkan:

1. Setiap *user* memiliki *User ID* dan *password* yang bersifat unik dan rahasia untuk mengakses sistem data dan informasi milik PLN. *User ID* dan *password* adalah tanggung jawab pribadi *user* dan tidak diperkenankan untuk berbagi dengan personel lain.
2. *User* harus memberitahukan *user administrator* mengenai perubahan status mereka di PLN untuk perubahan status *user*.
3. Semua akses yang diberikan kepada pihak non-PLN, terutama yang berkaitan dengan akses informasi dan sistem pendukung harus mendapatkan otorisasi dari manajemen terkait.

b. Pemberian akses *user*

Pemberian hak akses *user* harus dibatasi kepada personel yang berwenang sesuai dengan tanggung jawab pekerjaan, dan hak akses *user* hanya diberikan setelah mendapatkan persetujuan dari manajemen terkait. Hak akses yang diberikan perlu mempertimbangkan pemisahan tugas (*segregation of duties*) dan pemberian akses minimum sesuai dengan kebutuhan.

c. Pemakaian lisensi dalam manajemen *user*

PLN harus terlebih dahulu memastikan ketersediaan lisensi sebelum membuat atau memodifikasi *user*. PLN harus menyesuaikan posisi lisensi PLN untuk setiap pembuatan, modifikasi, dan penghapusan *user* pada sistem berlisensi.

d. Manajemen akses khusus

1. Kebutuhan hak akses khusus

Hak akses bagi semua *user*, sistem, dan program harus dibatasi secara tepat, diantaranya:

- Pertimbangan adanya kebutuhan untuk mengetahui hak akses.
- Hak akses khusus hanya boleh diberikan kepada dan digunakan oleh *user* yang sah sesuai dengan tujuan bisnis yang telah diamanatkan.
- Segala bentuk akses khusus terhadap sistem, seperti akun *superuser*, *root*, *administrator* tidak boleh digunakan untuk aktivitas operasional rutin atau sehari-hari.

2. User dengan hak akses khusus

Semua perangkat dan sistem jaringan harus mendukung *UserID* tipe tertentu yang memiliki hak khusus yang memungkinkan untuk mengubah kondisi keamanan sistem tersebut.

3. Jumlah *UserID* dengan hak akses khusus

Jumlah *UserID* dengan hak akses khusus harus dibatasi secara ketat hanya bagi yang sepenuhnya memiliki hak untuk kepentingan tujuan bisnis yang menjadi wewenangnya.

4. Menjalankan sistem *level command*

End user tidak diperkenankan untuk memiliki akses dan mengubah sistem *level command* dengan memberi batasan yang tepat sehingga hanya dapat menggunakan menu yang berisi fungsi-fungsi yang memang diperbolehkan untuk dijalankan.

5. Kontrol penggunaan hak akses khusus

Kontrol keamanan tambahan diperlukan dalam penggunaan hak akses khusus, terutama untuk aset data dan informasi yang bersifat rahasia. Penggunaan *user* dengan tipe ini membutuhkan persetujuan oleh *user* yang berwenang dan harus dipantau secara periodik.

e. Manajemen *password*

1. Manajemen *password user*

Password perlu diatur agar:

- Memiliki jangka waktu masa berlaku (kadaluarsa)
- Memiliki kriteria *password* sehingga hanya *password* berkualitas yang digunakan, seperti panjang minimum, kompleksitas *password*, dan mencegah penggunaan kembali *password* yang sama dengan beberapa *password* sebelumnya

2. Transmisi *password*

Password sedapat mungkin ditransmisikan melalui saluran komunikasi yang aman dan terenkripsi.

3. Lupa *password*

Semua user yang lupa atau tidak bisa menyatakan *password* mereka, harus segera melapor ke *service desk* atau administrator, pihak berwenang atau mekanisme yang diatur perusahaan untuk diberikan *password* sementara dan kemudian melakukan penyetelan ulang *password*.

4. Reset *password* setelah *locked out*

Semua sistem PLN yang menggunakan *password* saat *login* harus dikonfigurasi untuk membatasi usaha memasukkan *password* yang acak secara berturut-turut (*brute force attack*). Jika kegagalan login mencapai jumlah tertentu, *User ID* dinonaktifkan (*locked out*) dan hanya bisa di-reset oleh pihak berwenang atau mekanisme yang diatur perusahaan setelah melakukan otentifikasi identitas *user* yang bersangkutan.

5. Identifikasi penggunaan sistem

Semua *user* harus diidentifikasi sebelum diperbolehkan menggunakan perangkat atau sistem komunikasi multi *user* manapun.

f. Review akses *user*

Hak akses sistem yang diberikan kepada setiap *user* harus dievaluasi ulang pemilik proses bisnis secara berkala untuk memastikan kembali bahwa hak atau wewenang atas sistem yang diberikan tersebut memang masih diperlukan untuk menjalankan tugas pekerjaan. Review akses *user* juga dapat dilakukan kapanpun atas permintaan

manajemen, *information owner*, ISM atau audit.

g. Penghapusan dan penyesuaian hak akses

Dalam hal terjadi perubahan fungsi pekerjaan, atau status pekerja, hak akses user harus disesuaikan kembali atau dihapus sesuai dengan kebutuhan dan kewenangan pengguna.

9.3 Tanggung jawab *user*

9.3.1 Penggunaan *password*

Beberapa hal yang perlu diperhatikan dalam penggunaan *password*:

a. Struktur *password*

Password tidak boleh memiliki struktur atau karakter *password* yang membuatnya bisa diprediksi dan dengan mudah ditebak, misalnya sama dengan *UserID*, deret karakter yang lazim, ciri-ciri pribadi, atau identitas diri.

b. *Password* yang sering dipakai

User tidak boleh membuat *password* tetap yang mana menggabungkan karakter yang tidak berubah-ubah, dengan karakter lain yang perubahannya mudah ditebak.

c. Dugaan terungkapnya *password*

Setiap *user* harus mengubah *password* jika *user* memiliki kecurigaan atau menduga bahwa *password* tersebut telah terungkap atau diketahui oleh pihak yang tidak berwenang.

d. Tanggung jawab atas *UserID* dan *password*

User harus bertanggung jawab atas semua aktivitas yang dilakukan dengan *UserID* yang dimiliki dan tidak boleh membiarkan personel lain melakukan pekerjaan apapun dengan *UserID* miliknya, atau melakukan pekerjaan apapun dengan *UserID* milik personel yang lain. *Password* milik *user* harus terjaga kerahasiaannya dan tidak dicantumkan pada media fisik tanpa pengamanan yang memadai.

e. Berbagi kode akses

Kode akses yang dimiliki oleh PLN tidak boleh digunakan oleh pihak selain yang memang ditunjuk untuk menggunakannya.

f. Otentikasi pengguna

Otentikasi *user* yang lebih kuat dapat digunakan untuk melindungi aset data dan informasi yang memerlukan perlindungan tambahan.

9.4 Kontrol akses sistem dan aplikasi

9.4.1 Pembatasan akses informasi

Hak akses *user* (untuk *read*, *write*, *delete*, dan *execute*) pada sistem dan aplikasi perlu diatur sesuai dengan kewenangan dan kebutuhan pekerjaan. Kontrol pengamanan yang sesuai perlu diterapkan baik *logic* atau fisik untuk melindungi informasi sesuai dengan klasifikasi informasinya.

9.4.2 Prosedur *log on* secara aman

Beberapa hal yang perlu diperlatihkan tentang prosedur *log on*.

a. Proses akses ke perangkat

Akses ke perangkat PLN harus melalui proses otentikasi minimum seperti *UserID* dan *password*. *Password*, PIN dan sejenisnya harus disamarkan ketika ditampilkan di layar.

b. Percobaan *password* gagal

Apabila terdapat kesalahan pada saat *login*, sistem tidak menunjukkan jenis kesalahan yang dilakukan (misalnya, salah *UserID* atau salah *password*). Setelah tidak berhasil memasukkan *password* sebanyak jumlah tertentu, *UserID* yang bersangkutan harus ditahan untuk tidak dapat melakukan *login* terlebih dahulu secara sementara sampai ada permintaan untuk menyetel ulang *password* ke petugas yang berwenang. Sistem mempunyai toleransi jumlah kegagalan *login* sebelum *UserID* tersebut diblokir. Kegagalan *login* dicatat dalam *log* peristiwa keamanan.

c. Session *timeout*

Sistem harus menutup/menonaktifkan sesi koneksi yang tidak melakukan aktivitas selama periode waktu tertentu.

9.4.3 Sistem manajemen *password*

Sistem manajemen *password* perlu memastikan bahwa:

a. Pengaturan panjang *password*

b. Umur/retensi *password*.

c. *User* harus mengganti *password* yang lama dengan *password* yang baru ketika pertama kali *login*.

d. *Password* yang dibuat/dipilih harus berbeda dari beberapa *password* terakhir.

e. *Password* yang ditampilkan harus disembunyikan, atau ditutup untuk menghindari *password* dari pihak yang tidak berwenang.

- f. *Password* harus selalu dienkripsi pada saat disimpan, dan ditransmisikan melalui jaringan.
- g. *Default password* yang disediakan atau dibuat oleh mitra kerja harus diubah.
- h. Rumus, algoritma, formula dan informasi lain tentang proses pembuatan *password* harus dikontrol/ dilindungi secara ketat.

9.4.4 Pemakaian program *utility*

Program *utility* merupakan aplikasi atau *tools* yang memiliki kemampuan untuk *override* atau mengambil alih sistem yang ada. Ketentuan program *utility* yang perlu diperhatikan sebagai berikut. Proses kontrol yang diterapkan untuk penggunaan aplikasi atau tools yang memiliki kemampuan “*overriding*” dengan cara divalidasi, diidentifikasi kelemahan/kerentanannya, dipisahkan dengan aplikasi *software*, dilakukan tes *diagnostic*, dibatasi aksesnya dan diterapkan penggunaan *log*.

9.4.5 Akses ke kode program (*source code*)

Beberapa hal yang diperhatikan terkait akses ke *souce code*.

a. Kode program dan *library*

Kode program dan *library* sedapat mungkin tidak ditempatkan pada sistem produksi atau sistem operasional.

b. Pembatasan akses ke kode program.

Akses terhadap kode program dan *library* perlu dibatasi kepada personel tertentu yang memiliki kewenangan untuk mengelola kode program.

c. Manajemen perubahan kode program.

Segala bentuk perubahan pada kode program perlu diatur dan melalui prosedur yang telah ditetapkan, termasuk proses otorisasi untuk perubahan.

d. *Log* akses kode program

Akses ke kode program perlu dicatat atau di-*log*.

10 Kriptografi

10.1 Kontrol kriptografi

10.1.1 Kebijakan penggunaan kontrol kriptografi

Hal yang perlu dilakukan dalam penggunaan kriptografi:

a. Penggunaan kontrol kriptografi

Kriptografi harus digunakan untuk melindungi informasi rahasia atau sensitif, atau untuk memberikan kepastian keamanan dimana kontrol yang ada masih dianggap kurang memadai.

b. *Risk assessment* dalam penentuan kontrol kriptografi

Risk assessment dapat dilakukan sebelum menentukan kontrol kriptografi yang akan diterapkan, dimana tingkat risiko yang ada dapat menjadi pertimbangan dalam menentukan jenis, kekuatan, dan kualitas algoritma enkripsi yang digunakan.

c. Enkripsi dalam transfer informasi

Enkripsi perlu digunakan untuk informasi rahasia dan sensitif yang ditransfer secara *mobile*, melalui *removable media*, *device*, atau jaringan komunikasi.

d. Standar penerapan kriptografi

Penerapan kontrol kriptografi mengikuti standar yang ditetapkan oleh PLN atau mengikuti *best practice* yang berlaku.

10.1.2 Manajemen key (kriptografi)

Beberapa yang diperlukan dalam manajemen *key* (kriptografi):

a. Kontrol akses *logic key*

Key harus dilindungi secara *logic* dengan enkripsi atau kontrol akses *logic* lain.

b. Kontrol akses fisik *key*

Key dilindungi dengan akses fisik seperti *dual control*, serta penyimpanan *key* pada lokasi yang aman dan terkunci.

c. Pembuatan *key*

Pembuatan *key* harus menggunakan teknik acak yang tinggi (*random*) untuk mencegah *key* yang dihasilkan mudah ditebak.

d. Backup *key*

Backup atas *key* harus tersedia dan disimpan pada lokasi *off-site* yang aman.

e. Penggantian berkala *key*

Key harus diganti secara berkala untuk mengurangi risiko kemungkinan *key* diketahui atau ditebak oleh pihak tidak berwenang. Periode berlaku *key* juga perlu dibatasi. Apabila *key* dicurigai sudah tidak aman, atau telah diketahui pihak yang tidak berwenang, maka harus diganti secepatnya dari sistem atau layanan.

f. *Dual control atas key*

Key harus dikelola paling tidak oleh 2 (dua) orang yang berbeda untuk menghindari adanya penyalahgunaan. Setiap personel tersebut bertanggung jawab penuh atas keamanan key yang dimilikinya.

g. *Lokasi key*

Key harus ditempatkan pada lokasi penyimpanan yang terbatas.

Dalam pengelolaan key ini diperlukan adanya *key management system* (KMS).

10.1.3 Dukungan manajemen atas penerapan kriptografi

Dukungan dari manajemen harus diberikan untuk penerapan teknis kriptografi.

11 Keamanan fisik dan lingkungan

11.1 Secure area

Klasifikasi *secure area* atau zona pengamanan mengacu pada aturan yang ditetapkan oleh manajemen PLN.

11.1.1 Keamanan perimeter fisik

Berikut beberapa yang perlu diperhatikan terkait keamanan perimeter fisik.

a. *Lokasi secure area*

Perangkat data dan komunikasi harus ditempatkan di lokasi yang aman, misalnya: lantai atas suatu bangunan, jauh dari dapur dan pada ruangan yang tidak berbatasan langsung dengan dinding luar bangunan. Detil denah dan lokasi *secure area* sedapat mungkin dirahasiakan.

b. *Rencana keamanan fisik secure area*

Rencana pengamanan fisik untuk *secure area* harus dikaji ulang secara periodik sesuai dengan perkembangan dan kebutuhan bisnis.

c. *Kontrol perimeter fisik*

Kontrol perimeter yang tepat harus diterapkan dalam mengurangi risiko fisik yang berkaitan dengan aset data dan informasi, umumnya mencakup:

1. Pemisahan area dengan jelas yang dilindungi oleh dinding, lantai dan atap yang kokoh.
2. Terdapat area *reception* atau sejenisnya untuk membatasi akses dan melakukan otentifikasi terhadap tamu atau pengunjung.

3. Pintu keluar darurat harus dipasangi alarm yang aktif dan hanya dapat dibuka dari dalam.

11.1.2 Kontrol akses masuk

Beberapa ketentuan terkait kontrol akses masuk.

a. Pengamanan akses masuk

Area pengamanan asset data dan informasi harus diamankan dengan kontrol jalur masuk sehingga hanya dapat diakses oleh personel yang berwenang dan telah diotentikasi. Pengamanan dilakukan menggunakan perangkat atau teknologi yang sesuai untuk melakukan identifikasi, otentikasi, dan pemantauan akses masuk (misalnya, kartu akses, pemindai sidik jari, pemindai muka).

b. Otorisasi akses masuk non pegawai PLN

Pihak ketiga/tamu dapat diberikan akses terbatas ke *secure area* apabila dibutuhkan (misalnya untuk *maintenance/support*) setelah mendapatkan persetujuan sesuai prosedur yang berlaku.

c. Pencatatan dan pengawasan akses masuk

Nama, keperluan kunjungan, tanggal, jam masuk, dan jam keluar harus dicatat dalam buku tamu. Buku tamu dan *log* akses masuk perlu disimpan dan ditinjau secara berkala.

d. Tanda pengenal untuk identifikasi

Pekerja, pengunjung dan tamu harus selalu mengenakan tanda pengenal yang dapat dilihat dengan jelas selama berada di lokasi.

e. Review berkala atas akses masuk

Akses masuk ke *secure area* perlu ditinjau secara berkala untuk memastikan akses ke *secure area* hanya diberikan kepada yang berwenang.

11.1.3 Pengamanan kantor, ruangan, fasilitas di *secure area*

Hal-hal yang perlu diperhatikan meliputi:

a. Keamanan fasilitas perangkat data dan informasi serta komunikasi.

Fasilitas perangkat data dan informasi dan peralatan komunikasi harus diletakkan dalam ruang terkunci, termasuk:

1. Fungsi pendukung dan peralatan kantor seperti mesin fotokopi, printer, mesin fax harus ditempatkan pada lokasi yang aman dan jauh dari akses umum
2. Area kerja harus dalam keadaan terkunci apabila tidak digunakan, termasuk jendela/ruangan yang dapat diakses dari tempat umum

3. Kontrol terhadap penyusup (seperti sistem alarm, pendekripsi gerak atau CCTV) harus dipasang, diuji dan dipelihara.
- b. Tanda ruangan fasilitas perangkat data dan informasi serta komunikasi

Area atau lokasi fasilitas perangkat data dan informasi serta komunikasi sensitif harus ditempatkan pada area dengan akses publik seminimal mungkin, tidak mencolok dan tidak diberikan tanda yang menunjukkan lokasi dan keberadaannya. Peta, denah gedung, dan sebagainya yang mengidentifikasi lokasi fasilitas perangkat data dan informasi serta komunikasi yang sensitif tidak boleh diungkapkan kepada pihak eksternal kecuali diperlukan atas persetujuan manajemen PLN.

- c. Petugas keamanan

Petugas keamanan gedung bertanggung jawab untuk mengamankan lokasi, antara lain dengan cara:

1. Secara aktif mengawasi dengan berjalan mengelilingi gedung dan area kerja.
2. Memastikan bahwa keamanan fisik berjalan dengan baik.
3. Segera mengidentifikasi dan mengatasi masalah keamanan fisik.
4. Bertindak cepat menanggapi pelanggaran keamanan.

- d. Pengawasan alat pengintaian secara periodik

Pemeriksaan rutin dengan peralatan pengintaian dan peralatan perekaman pada seluruh lokasi fasilitas dan area kerja harus dilakukan.

11.1.4 Pengamanan terhadap bencana

Perlindungan fisik dan lingkungan perlu diterapkan untuk mengontrol dan memitigasi kerusakan yang disebabkan oleh api, banjir, gempa bumi, ledakan, aksi masa, dan berbagai bentuk bencana lainnya, termasuk kerusakan yang diakibatkan oleh manusia.

- a. Pengamanan bencana

Area yang diamankan seperti ruang komputer dan peralatan komunikasi harus memiliki tingkat perlindungan yang sesuai untuk meminimalkan kemungkinan dan dampak dari insiden seperti kebakaran, kebanjiran, gempa bumi, ledakan, kerusuhan, dan sebagainya, serta memenuhi persyaratan keselamatan kerja.

- b. Pengamanan terhadap kebakaran

Dalam mengurangi risiko dan dampak kebakaran, hal berikut perlu diperhatikan:

1. Pengamanan terhadap kebakaran pada secure area (khususnya sistem *fire extinguisher, water sprinkler*) harus dirancang, dan dipelihara dengan mempertimbangkan tingkat risikonya dan persyaratan khusus untuk secure area.
2. Alat pemadam kebakaran *portable* harus tersedia dan ditempatkan pada lokasi yang mudah dijangkau. Alat pemadam kebakaran portabel harus dipelihara dan diuji secara berkala.

3. Pekerja di secure area harus memahami cara menangani kebakaran termasuk merespon *alarm*, evakuasi peralatan, evakuasi manusia, serta mengendalikan kebakaran kecil.
4. Material yang mudah terbakar (seperti kardus, kertas) harus ditempatkan di luar *secure area*.
- c. Lokasi *disaster recovery center* (DRC)

Penentuan lokasi DRC harus didahului *feasibility study* untuk mengurangi risiko kerusakan pada saat yang bersamaan terjadinya risiko pada *main data center*.

11.1.5 Bekerja di *secure area*

Perlindungan fisik dan panduan untuk bekerja di *secure area* harus didesain dan diterapkan, diantaranya:

- a. Keberadaan, aktivitas, dan aset dalam *secure area* tidak boleh dipublikasikan secara umum. Informasi di atas hanya diberitahukan kepada pekerja yang memiliki wewenang untuk mengetahuinya.
- b. Pihak mitra kerja yang bekerja di *secure area* harus dibatasi, diawasi, dan sedapat mungkin didampingi. Sedangkan untuk pekerjaan yang dilakukan oleh pegawai dalam *secure area* juga sedapat mungkin diawasi.
- c. Area yang tidak digunakan harus dikunci dan secara rutin diperiksa oleh petugas yang bertanggung jawab.
- d. Perekaman gambar atau suara tidak boleh dilakukan di dalam *secure area* kecuali telah diizinkan sebelumnya.

Area *loading* dan *delivery*, area publik, seperti area pengiriman (*delivery*) dan bongkar-muat (*loading*) serta area lain yang dapat diakses pihak eksternal harus dikontrol dan diawasi untuk menghindari akses yang tidak sah. Area *loading* harus dibuat sedemikian rupa sehingga pihak yang tidak berwenang tidak dapat mengakses bagian lain dari gedung melalui area *loading* tanpa pemeriksaan dan pengawasan. Barang yang masuk harus diperiksa terhadap kemungkinan yang dapat membahayakan, dan dicatat sesuai dengan prosedur yang berlaku.

11.2 Peralatan

11.2.1 Keamanan dan penempatan peralatan

Beberapa hal yang perlu diperhatikan terkait keamanan dan penempatan peralatan, yaitu:

- a. Penempatan peralatan

Seluruh perangkat penyedia data dan informasi harus secara fisik terletak pada daerah yang aman sesuai klasifikasi *secure areanya*.

b. Kontrol lingkungan untuk peralatan

Untuk melindungi lingkungan tempat penempatan peralatan, pengendalian lingkungan perlu diterapkan seperti dengan adanya pendektsian dan pemadaman api, penyesuaian daya listrik, pengaturan temperatur udara, pengendali kelembaban, dan pengendalian lingkungan lainnya.

c. Pintu akses peralatan

Semua pintu pada akses perangkat penyedia data dan informasi harus selalu dikunci kecuali jika akan dilakukan perbaikan, pemeliharaan, atau perubahan konfigurasi.

d. Perangkat akses data dan informasi milik personal

Pegawai diperbolehkan membawa perangkat akses data dan informasi milik pribadi (perangkat keras dan perangkat lunak) ke dalam lokasi area penempatan peralatan PLN melalui persetujuan pihak yang berwenang atau ISM.

e. Larangan merokok, makan dan minum

Pegawai maupun pengunjung dilarang merokok (termasuk rokok elektronik), makan atau minum dalam area tempat penyimpanan peralatan penyedia data dan informasi.

11.2.2 Peralatan listrik cadangan

Dalam melindungi perangkat penyedia data dan informasi dari gangguan listrik dan gangguan lainnya maka perlu disediakan peralatan listrik cadangan yang memadai. Peralatan listrik cadangan harus mencukupi kebutuhan peralatan, dapat bekerja dalam jangka waktu yang diperlukan, harus diperiksa dan diuji secara berkala untuk memastikan dapat berfungsi saat dibutuhkan.

11.2.3 Keamanan perkabelan

Kabel listrik dan telekomunikasi yang membawa data atau mendukung pelayanan informasi harus dilindungi dari penyadapan (intersepsi), kerusakan atau pemutusan. Jalur komunikasi dan sumber listrik untuk peralatan pelayanan informasi yang kritis harus dibuat dengan redundansi untuk menghindari kegagalan *single point of failure*.

11.2.4 Pemeliharaan peralatan

Dalam pemeliharaan peralatan, hal yang diperhatikan meliputi:

a. Produk sistem data dan informasi

 Semua produk perangkat keras dan perangkat lunak harus segera didaftarkan ulang ke penyedia barang atau mitra kerja setelah diterima.

b. Pemeliharaan untuk pencegahan

Pemeliharaan pencegahan (*preventive maintenance*) harus secara teratur dilakukan pada seluruh perangkat penyedia data dan informasi serta peralatan komunikasi.

c. Pemeliharaan peralatan sistem data dan informasi

Semua peralatan sistem data dan informasi yang digunakan untuk kegiatan bisnis harus dirawat sesuai dengan interval waktu dan spesifikasi yang disarankan oleh mitra kerja. Perbaikan dan pemeliharaan peralatan hanya boleh dilakukan oleh personel yang berkompeten dan berwenang.

d. Pemeliharaan perangkat keras dan perangkat lunak penyimpan data

Perangkat keras dan perangkat lunak yang diperlukan untuk membaca media penyimpan data di arsip perusahaan harus tetap dipelihara agar selalu dalam kondisi yang siap dioperasikan.

e. Modifikasi perangkat penyedia data dan informasi

Perangkat penyedia data dan informasi yang disediakan oleh perusahaan, tidak diperkenankan untuk diubah, dimodifikasi, ditambah atau dikurangi dengan cara apapun tanpa melalui persetujuan Manajemen PLN.

f. Pencatatan pemeliharaan

Semua kerusakan, perbaikan, dan tindakan pemeliharaan harus dicatat dan dipantau.

g. Kontrol peralatan

Kontrol yang sesuai harus diterapkan apabila peralatan dibawa keluar dari area untuk diperbaiki.

h. Jaminan peralatan

Untuk peralatan yang dijaminkan, seluruh persyaratan yang diajukan oleh kebijakan penjamin harus dipatuhi dan ditaati.

11.2.5 Pemindahan peralatan

Hal yang perlu diperhatikan dalam pemindahan peralatan adalah:

a. Pemindahan peralatan oleh personel yang berwenang

Hanya personel yang berwenang atau yang diizinkan untuk membawa peralatan keluar/masuk dari/ke gedung kantor PLN. Personel tersebut bertanggung jawab penuh atas keamanan peralatan yang dibawa.

b. Persyaratan pemindahan

Perangkat yang terkait sistem data dan informasi, termasuk media penyimpanan data dan informasi tidak boleh dikeluarkan/dimasukan dari/ke lokasi kantor PLN kecuali jika disertai dengan formulir/dokumentasi dan persetujuan manajemen.

11.2.6 Keamanan peralatan dan aset di luar lokasi

Keamanan harus diterapkan untuk peralatan yang berada di luar kantor PLN dengan mempertimbangkan berbagai risiko, seperti:

- a. Peralatan dan media yang dibawa keluar dari area PLN tidak boleh dibiarkan tanpa pengawasan. Apabila di luar pengawasan, peralatan perlu ditempatkan pada lokasi yang terkunci.
- b. Mekanisme pengamanan fisik yang sesuai perlu diterapkan dengan mempertimbangkan risiko peralatan yang ditempatkan di luar area PLN
- c. Peralatan harus dilindungi sesuai dengan petunjuk penggunaan barang yang dikeluarkan oleh pabrik.

11.2.7 Pemusnahan atau penggunaan kembali peralatan secara aman

Hal yang perlu diperhatikan dalam pemusnahan atau penggunaan kembali peralatan meliputi:

- a. Peralatan yang rusak

Manajemen harus menetapkan apakah peralatan yang rusak yang berisi informasi sensitif dan rahasia harus dimusnahkan, diperbaiki, atau dibuang berdasarkan pertimbangan risiko.

- b. Pemusnahan peralatan dan media

Pemusnahan peralatan dan media (*disposal* perangkat keras dan perangkat lunak) yang tidak dapat digunakan atau tidak diperlukan lagi dalam aktivitas bisnis harus dilakukan sesuai dengan prosedur *secure deletion* atau *irreversible deletion* yang berlaku.

11.2.8 Peralatan tanpa pengawasan

User harus menjamin bahwa perangkat yang digunakan pada saat tertentu di luar kendali pengawasan, maka perangkat tersebut telah dilakukan pengamanan, misalnya:

- a. *Lock* atau *log-off* sesi aktif komputer, aplikasi, peralatan kelistrikan atau koneksi jaringan saat tidak sedang digunakan
- b. Pengamanan perangkat *mobile* dari akses yang tidak berwenang, seperti perlindungan password untuk *removable media*, atau *secure cable lock* untuk laptop

11.2.9 Kebijakan *clean desk* dan *clear screen*

Hal yang perlu diperhatikan dalam kebijakan *clean desk* dan *clear screen* sebagai berikut.

a. Kebijakan *clean desk*

Meja atau daerah kerja harus selalu bersih dari dokumen dan media *portable* (termasuk laptop) yang berisi informasi sensitif dan rahasia saat tidak digunakan atau saat pekerja tidak di tempat. Dokumen dan media tersebut harus disimpan dalam keadaan yang terkunci.

b. Kebijakan *clear screen*

Perangkat komputer atau terminal tidak boleh ditinggalkan tanpa pengawasan saat user sedang login, kecuali dalam keadaan terkunci (*locked*). Pekerja harus melakukan *log-off* komputer ketika semua sesi sudah selesai. Perangkat komputer harus dimatikan pada akhir hari kerja.

c. Printer, *faksimile*, dan fotokopi

Printer, mesin faksimile, mesin fotokopi dan semacamnya harus secara fisik lindungi dari akses tidak sah, umumnya dengan mengamankan ruangan kantor di mana peralatan tersebut berada. Semua dokumen yang dicetak pada *printer* atau mesin fotokopi harus dengan segera diambil oleh orang yang mencetaknya. Dokumen yang diterima melalui faksimile harus dengan segera diambil oleh petugas yang bertanggung jawab dan kemudian diteruskan kepada personel yang dituju dalam dokumen tersebut.

d. Pemusnahan dokumen

Dokumen dan kertas yang mengandung informasi yang sensitif dan rahasia perlu dihancurkan secara fisik dengan mesin penghancur kertas apabila sudah tidak lagi diperlukan.

12 Keamanan operasional

12.1 Prosedur dan tanggung jawab operasional

12.1.1 Dokumentasi prosedur operasional

Semua kebijakan dan prosedur operasional yang terkait dengan keamanan data dan informasi harus didokumentasikan, dikelola, dan diperbaharui secara berkala sesuai kebutuhan. Semua perubahan kebijakan dan prosedur harus mendapat persetujuan manajemen. Prosedur operasional yang didokumentasikan diantaranya:

- a. Pengelolaan dan penanganan aset data dan informasi
- b. Pengelolaan kontrol akses *logic*
- c. Pengelolaan kontrol kriptografi, termasuk enkripsi dan kunci enkripsi
- d. Pengelolaan akses area aman dan bekerja di area aman
- e. Pengelolaan akses jaringan, perangkat jaringan, dan layanan jaringan
- f. Manajemen pengembangan dan perubahan program

- g. Manajemen mitra kerja
- h. Manajemen insiden, termasuk proses eskalasi
- i. Manajemen keberlangsungan bisnis
- j. Pengelolaan kapasitas
- k. Prosedur pencegahan dan penanganan terhadap program berbahaya
- l. Prosedur *backup* dan *restore*
- m. Prosedur penanganan *error*, seperti *restart* dan *recovery* apabila terjadi kegagalan sistem
- n. Prosedur pengelolaan *scheduled job*
- o. Prosedur pemantauan aktivitas akses *logic* dan jaringan
- p. Prosedur pendukung operasional lainnya.

12.1.2 Manajemen perubahan

Beberapa hal yang diperhatikan terkait pengaturan manajemen perubahan data dan informasi sebagai berikut.

a. Otorisasi perubahan

Setiap perubahan, baik perubahan sistem maupun infrastruktur harus melalui otorisasi, pengujian, dan didokumentasikan. Perubahan tersebut harus dikendalikan sesuai dengan manajemen perubahan yang berlaku.

b. Pencatatan perubahan

Perubahan yang terjadi pada lingkungan produksi harus dicatat atau di-*log*.

c. Pengujian perubahan

Perubahan harus diuji coba terlebih dahulu sebelum diimplementasikan pada lingkungan produksi untuk menghindari dampak yang tidak diinginkan.

d. Dampak keamanan dari perubahan

Evaluasi atas keamanan sebagai dampak dari perubahan perlu dilakukan untuk memastikan perubahan tidak berdampak buruk terhadap keamanan.

e. Komunikasi perubahan

Informasi detail dari perubahan perlu dikomunikasikan atau dikoordinasikan dengan unit kerja atau unit bisnis yang terkait.

f. Kemampuan *roll back*

Strategi agar sistem dapat dipulihkan ke kondisi awal apabila terjadi kegagalan pada saat perubahan.

12.1.3 Manajemen kapasitas

Kebutuhan kapasitas harus dipantau dan selanjutnya diproyeksikan untuk memastikan kemampuan dan ketersediaan prosesor, memori, media, penyimpanan, perlengkapan komputer, dan sistem komunikasi untuk mempertimbangkan rencana perubahan sistem dan bisnis, serta tren kebutuhan di masa mendatang dalam menjamin terpenuhinya kinerja sistem yang diharapkan. Hasil pengawasan kapasitas perlu didokumentasikan dan dilaporkan secara berkala.

12.1.4 Pemisahan lingkungan pengembangan, pengujian, dan operasional

Hal-hal yang perlu diperhatikan dalam Pemisahan lingkungan pengembangan, pengujian, operasional sebagai berikut.

a. Pemisahan lingkungan produksi

Lingkungan produksi harus sepenuhnya terisolasi dari lingkungan pengembangan dan uji coba untuk mengurangi risiko insiden dan perubahan yang tidak diotorisasi pada lingkungan produksi. Apabila pemisahan secara fisik tidak dimungkinkan, maka harus diterapkan pemisahan secara *logic*.

b. Pemisahan lingkungan pengembangan dan lingkungan uji coba

Lingkungan produksi harus sepenuhnya terisolasi dari lingkungan pengembangan dan uji coba untuk mengurangi risiko insiden dan perubahan yang tidak diotorisasi pada lingkungan produksi. Apabila pemisahan secara fisik tidak dimungkinkan, maka harus diterapkan pemisahan secara *logic*.

c. Pemisahan lingkungan pengembangan dan lingkungan uji coba

Lingkungan pengembangan dan uji coba sedapat mungkin terisolasi satu sama lain, baik secara fisik ataupun *logic*.

d. Pemisahan peran

Personel yang ditugaskan dalam mengelola lingkungan pengembangan dan uji coba harus dipisahkan dengan personel yang ditugaskan untuk mengelola lingkungan produksi.

e. Migrasi ke lingkungan produksi

Pemindahan perangkat lunak baru atau perangkat lunak yang telah diubah ke lingkungan produksi harus dilakukan melalui prosedur perubahan yang berlaku.

f. Lingkungan uji coba

Lingkungan uji coba sedapat mungkin serupa dengan lingkungan produksi kecuali:

1. Personel yang memiliki *user* pada lingkungan pengembangan dan lingkungan uji coba tidak boleh mempunyai *user* pada lingkungan produksi

2. Data lingkungan produksi yang bersifat rahasia dan sensitif harus diganti terlebih dahulu dengan data *dummy* atau acak sebelum dipindahkan ke lingkungan pengembangan atau lingkungan uji coba.

12.2 Pengamanan dari *malware*

12.2.1 Kontrol terhadap *malware*

Hal-hal yang perlu diperhatikan dalam kontrol terhadap *malware* adalah:

- a. Kepatuhan lisensi perangkat lunak

Semua perangkat lunak yang digunakan dalam kegiatan operasional dan bisnis PLN harus diperoleh dari sumber yang terpercaya atau berlisensi.

- b. *Download* perangkat lunak

User tidak boleh mengunduh (*download*) perangkat lunak apapun tanpa persetujuan manajemen PLN.

- c. Pengamanan virus dan *malware*

Kontrol pengamanan terhadap virus dan *malware* perlu diterapkan, misalnya dengan penggunaan *antivirus* atau *antimalware*, yang harus di-*install* dan difungsikan pada semua perangkat *endpoint* PLN seperti komputer, laptop, tablet, dan smartphone dan dilakukan pembaruan secara berkala.

- d. Penanganan virus dan *malware*

Penanganan atas virus, *malware* dan program berbahaya lainnya dilakukan sesuai dengan prosedur yang berlaku.

- e. Pemulihan dari perangkat lunak berbahaya

PLN harus memiliki prosedur *recovery* yang mengatur kemampuan sistem informasi untuk memulihkan diri akibat dari perangkat lunak berbahaya yang merugikan.

- f. Pengamanan *file* berbahaya dari *e-mail* dan *web*

Pengamanan terhadap virus juga perlu diterapkan untuk mengurangi dan menanggulangi risiko *file* berbahaya yang berasal dari *e-mail*, *web* dan internet, misalnya dengan melakukan *scanning* virus dan *malware*. Pesan *e-mail* dari pengirim yang tidak dikenali, atau *file* yang bersumber dari website yang tidak jelas perlu segera dihapus dan tidak diteruskan kepada orang lain.

12.3 ***Backup***

12.3.1 ***Backup* data dan informasi**

Backup berkala perlu dilakukan terhadap semua data dan informasi bisnis yang bersifat penting dan perangkat lunak yang ada di dalam sistem PLN sesuai dengan kebutuhan. Informasi bisnis tersebut disalin ke dalam *disk*, *tape* atau media penyimpanan lain sesuai dengan *best practice* pengamanan data *back up*. Media penyimpanan tersebut harus selalu dalam keadaan baik untuk siap digunakan kapanpun untuk keperluan pengujian ataupun *restore*.

12.3.2 **Pengujian berkala *backup***

Hasil *backup* perlu secara berkala diuji coba untuk memastikan bahwa hasil *backup* dapat digunakan pada saat diperlukan. Uji coba tersebut juga harus memastikan bahwa *backup* dapat mengembalikan dan memulihkan layanan sesuai dengan kebijakan dan strategi *disaster recovery*.

12.3.3 **Penjadwalan *backup***

Setiap sistem informasi PLN harus mempunyai jadwal *back-up* masing-masing dalam rangka memenuhi persyaratan bisnis, persyaratan retensi atau persyaratan pemulihan data.

12.3.4 ***Backup off-site***

Backup dapat disimpan pada lokasi *off-site* yang aman untuk mengurangi dampak atas bencana yang terjadi pada lingkungan produksi, sesuai dengan kebutuhan dan hasil pengkajian risiko. Transportasi media *backup* dari dan ke fasilitas penyimpanan *off-site* mengikuti kebijakan pemindahan aset yang berlaku.

12.3.5 **Persyaratan minimum penyimpanan *backup***

Setiap perangkat penyimpanan data dan informasi harus memiliki kemampuan standar minimal yang ditetapkan oleh Manajemen PLN.

12.3.6 **Perlindungan *backup***

Backup harus dilindungi secara fisik dan *logic*. Perlindungan *backup* ini diterapkan untuk melindungi dari akses tidak sah, kebakaran, kerusakan fisik, tersiram air, pencurian, virus, *malware* dan sebagainya. Semua data dan informasi yang sensitif dan rahasia yang tersimpan dalam media *backup* harus dienkripsi.

12.4 Pencatatan *log* dan *monitoring*

12.4.1 *Monitoring* atas *log* penggunaan internet

Internet yang disediakan PLN adalah untuk keperluan yang mendukung bisnis dan aktivitas internasional, serta perlu dipantau penggunaannya untuk memastikan aktivitas internet selalu dalam keadaan aman

12.4.2 Pencatatan *log* kejadian

Sistem atau aplikasi yang dipakai dalam kegiatan bisnis dan operasional harus membuat *log* yang mencatat setiap penambahan, modifikasi, dan penghapusan data dan informasi sensitif tersebut di dalam sistem. Informasi yang disimpan dalam *log* sesuai dengan standar yang berlaku, dan disimpan sesuai dengan standar retensi penyimpanan informasi dalam membantu investigasi insiden keamanan dan *monitoring* aktivitas secara rutin.

12.4.3 Perlindungan atas *log*

Audit *log* harus selalu tersedia pada sistem atau aplikasi produksi. Fasilitas pencatatan *log* dan informasi *log* harus dilindungi dari sabotase dan akses yang tidak berwenang. Semua *log* sistem peralatan kegiatan bisnis PLN perlu dilindungi dengan mekanisme pengamanan yang tepat.

12.4.4 Log administrator dan operator

Semua sistem produksi *multi-user* PLN harus mempunyai *log administrator* dan *log* operator dimana memperlihatkan waktu aplikasi produksi mulai dan berhenti, waktu sistem *boot* dan *restart*, perubahan konfigurasi sistem, kesalahan sistem dan tindakan korektif yang diambil, dan konfirmasi bahwa *file* serta keluaran ditangani dengan tepat.

12.4.5 Review *log*

Semua *log* sistem produksi *multi-user* harus secara teratur di-review oleh staf teknis spesialis yang ditunjuk.

12.4.6 Sinkronisasi waktu

Waktu pada seluruh sistem pemrosesan informasi dan perangkat keamanan data dan informasi yang kritikal terhadap PLN atau kritikal terhadap keamanan perlu sinkron dengan suatu sumber pencatatan waktu yang telah disetujui.

12.5 Kontrol atas *software* operasional

12.5.1 Instalasi *software* pada sistem operasional

Instalasi *software* pada sistem operasional atau sistem produksi perlu dikontrol, antara lain:

- a. *Update software* operasional, aplikasi, dan *library* program dilakukan oleh personel yang ditunjuk dengan persetujuan manajemen yang berwenang
- b. Pengujian perlu dilakukan sebelum implementasi *software* pada lingkungan produksi
- c. Dokumentasi yang memadai, termasuk pencatatan dan *log* instalasi atau perubahan perlu disimpan dan dikelola.
- d. Sistem operasional tidak menyimpan kode program dan *compiler*.

12.6 Kerentanan teknis

12.6.1 Pengendalian kerentanan teknis

PLN harus mendapatkan informasi yang tepat waktu mengenai kerentanan teknis yang dapat berdampak pada keamanan sistem informasi, dengan cara:

- a. Melakukan *vulnerability assessment* dan/atau *penetration testing* terhadap sistem informasi serta infrastruktur komputer dan jaringan PLN.
- b. Kerentanan teknis yang ada perlu dikaji risikonya untuk menentukan langkah perubahan/ perbaikan yang sesuai (seperti *patching*, atau implementasi kontrol keamanan lainnya).
- c. *Patch* perlu diuji dan dievaluasi sebelum diimplementasikan untuk memastikan *patch* tidak mengganggu lingkungan produksi.
- d. Hasil pengkajian dan keputusan manajemen risiko dalam menganggapi kerentanan teknis harus dicatat, di-review, dan dipelajari untuk referensi dan pembelajaran di kemudian hari.
- e. Review atas kerentanan teknis harus dilakukan secara berkala atau setelah perubahan yang signifikan pada infrastruktur sistem.

12.6.2 Pembatasan instalasi *software*

User hanya diperkenankan untuk melakukan instalasi atau menggunakan perangkat lunak yang disediakan atau disetujui oleh Manajemen PLN.

User tidak diperkenankan untuk melakukan instalasi *software* ilegal (bajakan). Pelanggaran terhadap ketentuan ini mengikuti ketentuan yang berlaku.

12.7 Pertimbangan audit sistem data dan informasi

12.7.1 Kontrol audit sistem data dan informasi

Beberapa hal yang diperhatikan terhadap kontrol audit sistem data dan informasi.

a. Rencana audit

Manajemen PLN memiliki tanggung jawab pelaksanaan keamanan data dan informasi, serta menetapkan rencana audit informasi dan sistem pendukung.

b. Ruang lingkup audit

Ruang lingkup audit perlu disetujui oleh Manajemen PLN dengan fungsi yang berkaitan dengan lingkup audit.

c. Kebutuhan akses sistem oleh auditor

Kebutuhan akses ke dalam sistem dan kebutuhan data/informasi untuk keperluan audit perlu disetujui oleh manajemen yang berwenang. Akses yang diberikan hanya *read-only*.

d. Kebutuhan proses khusus untuk audit

Permintaan untuk proses khusus atau proses tambahan (misalnya *audit utility, test script*) pada lingkungan produksi harus disetujui oleh Manajemen PLN.

e. Pemeriksaan kepatuhan keamanan data dan informasi

Audit internal harus melakukan pemeriksaan kepatuhan (*compliance*) secara berkala terhadap semua kebijakan, standar, dan prosedur keamanan data dan informasi.

f. Perlindungan informasi dan sistem selama audit

Informasi dan sistem pendukungnya harus selalu terlindungi (diproteksi) termasuk didalamnya ketika dilakukan audit terhadap sistem tersebut.

13 Keamanan komunikasi

13.1 Manajemen keamanan jaringan

13.1.1 Kontrol jaringan

Hal-hal yang perlu diperhatikan dalam kontrol jaringan sebagai berikut.

a. Akses user jaringan

Akses ke dalam sistem dan jaringan data dan informasi PLN harus disetujui oleh Manajemen PLN dan didokumentasikan. Dokumentasi diperlakukan sebagai dokumen rahasia dan dilindungi secara memadai.

b. Konfigurasi keamanan

Semua perangkat yang dihubungkan ke jaringan PLN harus mematuhi kebijakan-kebijakan keamanan serta dikonfigurasi sesuai standar yang dikeluarkan Manajemen PLN.

c. *Logging* dan *monitoring*

Mekanisme *logging* dan *monitoring* perlu diterapkan untuk seluruh lalu lintas jaringan, termasuk pencatatan informasi keamanan, serta notifikasi atau peringatan atas kejadian penyimpangan. *Monitoring* lalu lintas jaringan data dan informasi yang disediakan untuk *user* harus dipantau secara rutin untuk mendeteksi adanya potensi insiden keamanan.

d. Transmisi informasi rahasia

Informasi rahasia dan sensitif yang dikirimkan melalui jaringan publik dan jaringan *wireless* harus dienkripsi atau menggunakan metode pengamanan lain yang memadai.

e. Jalur komunikasi ganda

Sistem komunikasi PLN harus dirancang sedemikian rupa agar komunikasi aplikasi yang kritis dapat segera dikirim melalui media komunikasi alternatif lain dan tidak bergantung pada satu penyedia saja.

f. Informasi jaringan internal

Informasi dan data terkait alamat, konfigurasi, dan informasi rancangan sistem yang terkait sistem internal pada sistem komputer dan jaringan PLN harus dibatasi untuk kalangan internal.

g. Pengamanan dengan perangkat keamanan

Perangkat keamanan perlu didesain untuk melindungi jaringan internal dari ancaman luar, diantaranya:

1. Semua sistem dan jaringan komputer PLN harus dilindungi oleh perangkat sistem pendeteksi gangguan (*intrusion prevention system*) dan *firewall*.
2. Perangkat keamanan harus dikonfigurasi dengan konsep pertahanan berlapis dan konsep *failsafe operation* (misalnya *default deny*)
3. Semua applet masuk yang mengandung *active content* harus secara otomatis dihilangkan oleh *firewall*.
4. Semua akses internet menggunakan komputer di kantor PLN harus melewati *firewall*.

5. Gerbang antar muka (*gateway*) jaringan *wireless* harus selalu dikonfigurasi sehingga selalu menggunakan *firewall* untuk menyaring komunikasi dengan perangkat lain.
 6. Konfigurasi dan aturan-aturan layanan yang diberlakukan pada *firewall* harus mengikuti prosedur yang berlaku.
- h. Server internet publik
- Server internet publik harus ditempatkan pada jaringan yang terpisah dari jaringan internal PLN. Lalu lintas dari dan ke publik harus selalu dibatasi oleh *router* atau *firewall*.
- i. Koneksi jaringan dengan organisasi eksternal
- Koneksi antara sistem atau perangkat komputer PLN dengan organisasi eksternal melalui internet atau jaringan publik lain harus melalui persetujuan Manajemen PLN.
- j. Perubahan jalur komunikasi
- Pekerja dan mitra kerja dilarang mengubah susunan, atau melengkapi instalasi saluran suara atau data dengan perusahaan telekomunikasi manapun tanpa persetujuan Manajemen PLN.
- k. Kriteria keamanan koneksi intranet
- Semua perangkat komputer dan segmen jaringan harus memenuhi kriteria keamanan yang ditetapkan oleh Manajemen PLN sebelum dapat dihubungkan ke jaringan internal PLN.
- l. Koneksi *remote*
- User dapat melakukan koneksi *remote* melalui internet/intranet menggunakan *best practice* keamanan secara terkontrol, terkendali dan terbatas sesuai kebutuhan bisnis atas persetujuan Manajemen PLN.
- m. Pemisahan tanggung jawab keamanan jaringan
- Tanggung jawab pengelolaan atau pengamanan jaringan sedapat mungkin dipisahkan dengan tanggung jawab pengelolaan atau pengamanan perangkat. Walaupun demikian, aktivitas kedua bagian tersebut harus dikoordinasikan untuk mengurangi risiko bisnis dan memastikan kontrol keamanan data dan informasi dijalankan secara konsisten pada seluruh infrastruktur.

13.1.2 Keamanan layanan jaringan

Hal yang diperhatikan dalam keamanan layanan jaringan:

- a. Pengamanan layanan jaringan

Koneksi ke layanan jaringan perlu dilakukan dengan menerapkan kontrol yang memadai, seperti mekanisme otentikasi, enkripsi, dan kontrol keamanan lainnya.

b. Inventarisasi perangkat jaringan

Persediaan cadangan perangkat jaringan harus selalu tersedia.

c. Otorisasi koneksi perangkat jaringan

Otorisasi terhadap user harus dilakukan sebelum dapat menggunakan perangkat jaringan.

d. *Monitoring* layanan jaringan mitra kerja

Kemampuan mitra kerja penyedia layanan jaringan dalam mengamankan jaringan harus di-review secara berkala. Oleh karena itu, hak untuk melakukan audit perlu dicantumkan dalam perjanjian kerjasama.

13.1.3 Pemisahan jaringan

Faktor-faktor keamanan harus dipertimbangkan ketika merancang, mengkonfigurasi, atau mengubah arsitektur jaringan. Sistem dan jaringan internal PLN harus dipisahkan sesuai dengan risiko pengamanan informasi ke dalam kategori, kelompok, atau domain terpisah seperti:

- a. Jaringan eksternal (seperti internet) dipisahkan dari jaringan internal.
- b. Sistem yang dimiliki atau dikelola oleh pihak ketiga dipisahkan dari sistem yang dimiliki atau dikelola oleh PLN.
- c. Lingkungan untuk pengembangan, uji coba dan produksi harus dipisahkan.
- d. Jaringan dengan kabel dipisahkan dengan jaringan nirkabel.
- e. Lalu lintas jaringan *user* dipisahkan dari lalu lintas jaringan pengelolaan sistem dan pengelolaan jaringan.
- f. Pemisahan atau segmentasi jaringan mengacu kepada arsitektur yang ditetapkan oleh Manajemen PLN dan sesuai *best practice* keamanan.

13.1.4 Dokumentasi jaringan

Seluruh koneksi jaringan (meliputi diagram, struktur dan konfigurasi jaringan) harus didokumentasikan dan menggambarkan kondisi saat ini.

13.2 Transfer data dan informasi

13.2.1 Kebijakan dan prosedur keamanan transfer data dan informasi

Standar dan prosedur pertukaran data dan informasi harus ditetapkan untuk melindungi transfer data dan informasi, antara lain:

- a. Penggunaan teknik kriptografi untuk melindungi kerahasiaan, integritas, dan keaslian informasi berdasarkan klasifikasi data dan informasi
- b. Dalam pertukaran data dan informasi melalui media elektronik dipastikan perangkat terlindungi dari program berbahaya (contoh: virus, *malware*)
- c. Ketentuan *acceptable user* terkait penggunaan fasilitas komunikasi elektronik perlu dibuat dan diterapkan
- d. Pekerja dan mitra kerja tidak diperkenankan untuk mengirimkan *e-mail* untuk tujuan serangan, mengirimkan *e-mail* spam, meneruskan *e-mail* berantai, dan lain sebagainya yang dapat merugikan PLN.
- e. Masa retensi dan pemusnahan pertukaran data dan informasi dalam hubungan bisnis (termasuk *e-mail*) harus sesuai dengan kebutuhan bisnis, mematuhi hukum dan ketentuan yang berlaku di PLN.
- f. Media pertukaran data dan informasi PLN yang mengandung informasi rahasia dan sensitif tidak diperkenankan untuk diteruskan ke pihak eksternal.
- g. Setiap pekerja PLN tidak diperkenankan untuk membicarakan informasi sensitif dan rahasia di tempat umum, termasuk mengirim dokumen sensitif dan rahasia melalui layanan publik, seperti layanan *e-mail* di luar PLN, *public file sharing* dan media data lainnya.

13.2.2 Ketentuan transfer data dan informasi

Hal-hal yang perlu diperhatikan dalam ketentuan transfer data dan informasi.

- a. Kesepakatan pertukaran data dan informasi dengan mitra kerja

Sebelum pertukaran informasi dilakukan dengan mitra kerja, perlu ada kesepakatan terlebih dahulu perihal kontrol dan notifikasi pada saat informasi dikirimkan, ditransmisikan, hingga informasi tersebut diterima.

- b. Distribusi perangkat lunak pada mitra kerja

Semua perangkat lunak yang dikembangkan oleh PLN yang akan digunakan oleh pelanggan, mitra bisnis, dan pihak luar lainnya harus didistribusikan setelah melalui persetujuan Manajemen PLN.

- c. Perjanjian perangkat lunak mitra kerja

Semua perangkat lunak yang dikembangkan oleh PLN yang akan digunakan oleh pelanggan, mitra bisnis, dan pihak luar lainnya harus didistribusikan setelah mitra kerja menandatangani perjanjian yang menyatakan mereka tidak akan membongkar, merekayasa ulang, memodifikasi, atau tidak menggunakan program kecuali setelah mendapat persetujuan Manajemen PLN.

d. Perjanjian perubahan perangkat lunak dan data

Pertukaran perangkat lunak *in-house* atau informasi internal antara PLN dan mitra kerja manapun harus disertai satu perjanjian tertulis yang menspesifikasikan syarat-syarat pertukaran, dan cara perangkat lunak atau informasi ditangani serta diproteksi.

e. Jaminan penghancuran informasi

Ketika pihak eksternal mengembalikan informasi atau media penyimpanan data dan informasi yang telah diberikan atau dipinjamkan oleh PLN sebelumnya, pihak tersebut harus menyediakan pernyataan tertulis yang menyatakan bahwa semua salinan dari informasi tersebut telah dihancurkan.

f. Validasi identitas mitra kerja

Sebelum pegawai memberikan informasi internal PLN, atau memasukkan informasi tersebut ke dalam perjanjian, atau memesan produk melalui jaringan publik, identitas individu dan organisasi yang dihubungi tersebut harus dikonfirmasi melalui surat, *digital signature*, *letter of credit*, referensi mitra kerja, atau percakapan telepon.

13.2.3 Pesan elektronik

Hal-hal yang perlu diperhatikan dalam pesan elektronik meliputi:

a. Perlindungan pesan elektronik

Informasi dan pesan elektronik harus dilindungi sesuai dengan risiko dan klasifikasi informasi. Informasi rahasia dan sensitif harus dienkripsi ketika ditransmisikan melalui media elektronik, kecuali jika telah mendapatkan persetujuan manajemen untuk pengecualian.

b. Informasi pengirim pesan elektronik

Semua pesan elektronik yang dikirimkan menggunakan sistem yang disediakan oleh PLN harus menyertakan informasi pengirim, seperti nama, jabatan, dan unit organisasi.

c. Penerima pesan elektronik

Pesan elektronik harus disampaikan kepada penerima yang terpercaya dan dikenali. *User* harus memastikan alamat pesan elektronik ditujukan kepada penerima yang benar.

d. Alamat pesan elektronik

Dalam berkorespondensi menggunakan media elektronik untuk menunjang bisnis, pegawai PLN dilarang menggunakan alamat media elektronik selain alamat resmi PLN.

e. Penggunaan pesan elektronik

Pekerja dilarang membuat atau mengirim, atau meneruskan pesan elektronik yang berasal dari eksternal atau internal yang berisi informasi yang tidak sesuai dengan kebutuhan bisnis, hukum, dan ketentuan yang berlaku di Indonesia. Lebih lanjut, pekerja dilarang menggunakan sistem informasi PLN untuk mengambil bagian dalam kelompok diskusi internet, ruang chat, atau forum elektronik umum lainnya kecuali jika telah mendapat persetujuan dari Manajemen PLN.

f. Penanganan pesan elektronik

Administrator sistem PLN harus secara sistematis menetapkan dan memelihara proses *backup* data pesan elektronik sesuai dengan kebutuhan bisnis, hukum dan ketentuan yang berlaku di Indonesia. Lebih lanjut, pelindungan atas *spam* perlu diterapkan untuk layanan pesan elektronik.

g. Retensi pesan elektronik

Pesan surat elektronik harus dapat disimpan sebagai referensi di masa datang apabila: berisi informasi yang relevan untuk penyelesaian transaksi bisnis, berisi informasi referensi yang berpotensi penting, atau yang bernilai sebagai bukti keputusan manajemen PLN. Penyimpanan ini harus sesuai dengan kebutuhan bisnis, hukum, dan ketentuan yang berlaku di PLN.

h. Modifikasi pesan elektronik

Pegawai tidak diperbolehkan untuk memodifikasi atau menghilangkan informasi apapun dalam satu pesan surat elektronik termasuk *body of the message* (badan pesan) atau bagian awal (*header*).

i. Penghancuran pesan elektronik

Periode penghapusan log surat elektronik harus sesuai dengan kebutuhan bisnis, hukum, dan aturan yang berlaku di Indonesia.

j. Pesan elektronik yang mencurigakan

Pegawai PLN harus dengan segera melapor kepada personel yang ditunjuk dengan persetujuan manajemen yang berwenang apabila menerima pesan elektronik yang mencurigakan dan tidak melakukan respon terhadap pesan tersebut hingga mendapat konfirmasi.

k. *Monitoring* pesan elektronik

Administrator pesan elektronik wajib memberitahu setiap pemakai bahwa: sistem pesan elektronik hanya digunakan untuk tujuan bisnis, semua pesan yang dikirim dengan surat elektronik merupakan catatan PLN, PLN memiliki hak untuk mengakses dan mengungkapkan semua pesan tanpa pemberitahuan terlebih dahulu, serta dapat mereview untuk menentukan apakah telah terjadi pelanggaran keamanan, melanggar kebijakan perusahaan, atau tindakan yang tidak sah lainnya.

I. Pengarsipan dan *review* pesan elektronik

Semua pesan elektronik yang dikirim melalui layanan yang disediakan oleh PLN harus diarsipkan dengan tujuan untuk *di-review* oleh seseorang selain penerima serta pengirim.

m. Lampiran pesan elektronik

Pegawai dilarang membuka pesan elektronik berikut lampirannya kecuali jika dari sumber pengirim yang diketahui dan dipercaya, dan jika *attachment* telah di-scan oleh perangkat lunak *antivirus*.

n. Persetujuan pemantauan pesan elektronik

Administrator pesan elektronik tidak diperbolehkan melihat isi surat elektronik dengan alasan untuk pemenuhan kebijakan internal, memantau aktivitas kriminal yang mencurigakan, dan alasan lainnya kecuali mendapat penugasan khusus dan disetujui oleh manajemen.

o. Privasi pesan elektronik

Pesan elektronik merupakan informasi pribadi dan harus ditangani sebagai sebuah komunikasi pribadi antara pengirim serta penerima.

13.2.4 Perjanjian kerahasiaan (*non-disclosure agreement*)

Pertukaran informasi antara PLN dengan mitra kerja harus diatur dalam perjanjian kerjasama yang disetujui oleh kedua belah pihak dan berisi tanggung jawab serta kontrol yang diperlukan, diantaranya:

- a. Definisi informasi yang perlu diproteksi (misal, informasi rahasia)
- b. Periode atau jangka waktu berlakunya perjanjian
- c. Tanggung jawab untuk melindungi kerahasiaan informasi dan mencegah pengungkapan informasi yang tidak sah
- d. Kepatuhan terhadap hak milik informasi, hak milik intelektual, hak cipta, hak paten, merek dagang, dan hak lain yang sejenis
- e. Hak untuk melakukan pengawasan atau audit dalam aktivitas yang berkaitan dengan informasi rahasia
- f. Tanggung jawab dan kewajiban mitra kerja apabila terjadi insiden keamanan data dan informasi, misalnya kehilangan data atau pengungkapan data
- g. Tindakan yang diambil apabila perjanjian dicabut, dihentikan, atau dilanggar oleh salah satu pihak

14 Akuisisi, pengembangan dan pengelolaan sistem informasi

14.1 Kebutuhan keamanan sistem informasi

14.1.1 Analisis dan spesifikasi kebutuhan keamanan data dan informasi

Analisis dan spesifikasi kebutuhan keamanan data dan informasi meliputi:

a. Identifikasi persyaratan keamanan

Sebelum sistem baru dikembangkan atau dibuat, persyaratan dan spesifikasi keamanan perlu didefinisikan terlebih dahulu, dengan setidaknya mempertimbangkan:

1. Mekanisme perlindungan informasi (misal: kriptografi) untuk memastikan *availability*, *confidentiality* dan *integrity*, terutama untuk informasi yang bersifat sensitif dan rahasia seperti *password*.
2. Kontrol dan pembatasan akses *user*.
3. Kontrol pembatasan kriteria *password* yang dipilih.
4. Pencatatan *log* dan audit *trail*.
5. Persyaratan spesifik yang berasal dari kebutuhan proses bisnis, dan regulasi.
6. Persyaratan keamanan yang telah didefinisikan tersebut perlu diterapkan dan diaplikasikan pada saat pengembangan sistem informasi.

b. Spesifikasi pengembangan perangkat lunak

Semua perangkat lunak yang dikembangkan secara *in-house* yang diperuntukkan untuk mengolah informasi yang sensitif atau rahasia, harus mempunyai spesifikasi formal tertulis yang merupakan bagian dari perjanjian antara pemilik informasi dan pengembang sistem yang terlibat, kemudian *draft* harus dibuat dan disetujui sebelum pengembangan.

c. Teknik pengembangan perangkat lunak

Semua pengembangan perangkat lunak secara *in-house* harus menggunakan standar-standar dan teknik-teknik pengembangan perangkat yang telah matang dan teruji.

d. Keamanan dalam siklus pengembangan sistem

Untuk semua sistem aplikasi bisnis, perancang dan pengembang sistem harus mempertimbangkan keamanan dari awal proses perancangan sistem melalui konversi pada sistem yang digunakan pada kegiatan bisnis PLN.

e. Prinsip dan praktik *secure coding*

Prinsip dan praktik *secure coding* perlu dibuat dan diperbaharui oleh manajemen keamanan data dan informasi serta diimplementasikan untuk semua perangkat lunak yang dikembangkan atau dikelola secara *in-house*.

f. Pembelian solusi keamanan data dan informasi

PLN sebaiknya menerapkan solusi keamanan data dan informasi yang secara komersial sudah teruji baik dipasar dibanding membangun solusi *in-house*, kecuali jika efektivitas dan efisiensi biaya dari solusi *in-house* telah diteliti, dirancang, diuji, didokumentasikan, dan disetujui oleh ISM.

g. Penggunaan produk yang telah dievaluasi

Produk keamanan sistem informasi yang sudah dievaluasi secara resmi telah teruji, sebaiknya digunakan dibanding dengan produk yang belum pernah dievaluasi.

14.1.2 Pengamanan layanan aplikasi pada jaringan publik

Setiap layanan aplikasi yang tersedia di jaringan publik perlu dilindungi dari risiko (seperti penipuan, perselisihan perjanjian kerjasama, pengungkapan informasi tidak sah, modifikasi informasi, *denial of service*, kesalahan publikasi) melalui implementasi kontrol keamanan yang sesuai, seperti kontrol hak akses dan *digital certificate* sesuai dengan persyaratan bisnis dan hukum yang berlaku.

14.1.3 Pengamanan transaksi layanan aplikasi

Hal-hal yang perlu diperhatikan dalam pengamanan transaksi layanan aplikasi sebagai berikut.

a. Pengamanan transaksi

Informasi dalam transaksi *online/realtme* harus dilindungi dari pengiriman data yang tidak lengkap, salah tujuan, perubahan, penggandaan, pengulangan atau pengungkapan yang tidak sah, misalnya dengan menggunakan *digital certificates*, *digital signatures*, atau enkripsi.

b. Protokol yang aman

Jalur komunikasi layanan *online* harus menggunakan protokol yang aman.

c. Manajemen *digital signature/certificate*

Dalam hal penggunaan layanan jasa pihak ketiga (misalnya untuk membuat dan memelihara *digital signature*, dan/atau *digital certificate*) seluruh proses manajemen *certificate/ signature* harus dikelola dan dikontrol secara memadai.

14.2 Keamanan dalam proses pengembangan

14.2.1 Kebijakan keamanan dalam pengembangan

Kebijakan keamanan dalam pengembangan meliputi:

a. Kesadaran keamanan untuk pengembang

Kesadaran perihal keamanan perlu diberikan kepada seluruh pengembang aplikasi agar memiliki pengetahuan tentang standar-standar keamanan program, mengetahui tren terkini dalam hal keamanan dan privasi, serta memiliki kemampuan untuk menghindari, menemukan, dan memperbaiki celah-celah keamanan.

b. Persyaratan keamanan

Persyaratan keamanan untuk aplikasi perlu ditentukan sebelum pengembangan program, misalnya pada tahapan perencanaan atau desain.

c. Panduan *secure coding*

Pengembangan program dilakukan dengan mempertimbangkan aspek-aspek keamanan, menghindari celah kerentanan keamanan, serta mengikuti ketentuan *secure coding* yang telah ditetapkan.

d. Pengujian keamanan

Sistem yang dikembangkan harus diverifikasi kembali untuk memastikan sistem telah memiliki fitur keamanan dan memiliki fungsionalitas sesuai dengan yang telah didefinisikan sebelumnya.

e. Keamanan dalam proses manajemen perubahan

Mekanisme pengendalian yang tepat perlu diterapkan pada hasil dari seluruh tahapan pengembangan program, seperti dokumentasi pengembangan dan kode program.

14.2.2 Prosedur kontrol pengembangan dan perubahan sistem

Prosedur kontrol pengembangan dan perubahan sistem meliputi:

a. Pengujian perangkat lunak dan informasi

Sebelum mendistribusikan perangkat lunak atau informasi apapun secara elektronik ke pihak non-PLN, staf PLN yang berkompeten harus telah melakukan pengujian terhadap perangkat lunak atau informasi tersebut, termasuk melakukan *scanning virus* secara komprehensif.

b. Pemakaian *resource komputer*

Seluruh pekerja tidak diperkenankan untuk menjalankan atau menulis program atau proses komputer yang dapat mengganggu aktivitas bisnis PLN atau membebani sistem operasional.

c. Konvensi pengembangan sistem

Manajemen harus memastikan bahwa semua aktivitas pengembangan dan pemeliharaan perangkat lunak dilaksanakan oleh staf *in-house* berpegang pada kebijakan, standar, prosedur dan ketentuan pengembangan sistem yang ada.

d. Jalur akses pada produksi perangkat lunak

Sebelum mengaplikasikan perangkat lunak yang telah dikembangkan *in-house* ke lingkungan produksi, pemrogram dan staf teknis lainnya harus terlebih dahulu menghilangkan semua jalur akses dan hak akses istimewa khusus.

e. Fungsionalitas sistem

Fungsi yang dapat dijalankan pada komputer produksi atau sistem komunikasi yang dikembangkan *in-house* hanya merupakan fungsi yang telah didefinisikan dalam dokumen desain yang telah disetujui.

f. Penerapan prosedur kontrol perubahan

Semua sistem komputer dan komunikasi yang digunakan untuk proses kegiatan bisnis PLN harus menerapkan prosedur kontrol perubahan formal untuk mengotorisasi semua perubahan penting pada perangkat lunak, perangkat keras, jaringan komunikasi, dan prosedur terkait.

g. Dokumentasi kontrol perubahan

Dokumentasi selama proses kontrol perubahan aplikasi kegiatan bisnis harus dikelola secara memadai, menunjukkan apa yang diubah, bagaimana, personel yang membuat perubahan, personel yang menguji perubahan, personel yang memberikan otorisasi perubahan, personel yang melakukan migrasi ke lingkungan produksi, serta mengizinkan perubahan versi.

h. Notifikasi permasalahan sistem

Para perancang dan pengembang sistem secara individual bertanggung jawab untuk memberitahu manajemen proyek mengenai permasalahan yang mungkin timbul sebagai akibat dari aplikasi yang mereka buat atau modifikasi.

i. Pertimbangan keamanan dalam pengubahan sistem produksi

Mekanisme setiap pengubahan bukan darurat pada sistem produksi harus dapat ditunjukkan konsisten dengan arsitektur keamanan data dan informasi dan disetujui oleh manajemen sebagai bagian proses kontrol pengubahan formal.

j. Perangkat lunak yang tidak diperlukan

Fitur perangkat lunak yang tidak diperlukan harus dinonaktifkan ketika di-*install* pada sistem *multi-user*.

k. Pelatihan dan dokumentasi pengoperasian

Sistem aplikasi bisnis yang baru dikembangkan, atau mengalami modifikasi yang penting atau signifikan memerlukan materi pelatihan dan dokumentasi pengoperasian yang memadai.

I. Peninjauan ulang dan kompilasi ulang *software*

Modul perangkat lunak yang telah diuji sepenuhnya harus ditinjau dan dikompilasi ulang sebelum dimasukkan ke *library* sistem produksi.

m. Proses kontrol perubahan aplikasi bisnis

Perangkat lunak bisnis yang diimplementasikan pada sistem produksi harus mengikuti proses kontrol manajemen perubahan secara formal, termasuk mendapatkan otorisasi oleh manajemen sistem informasi dan manajemen organisasi pengguna.

n. Pengujian keamanan teknikal

Perangkat lunak yang dikembangkan atau dimodifikasi perlu diuji untuk memastikan kontrol dan prosedur keamanan di dalam sistem tetap berjalan, serta melakukan pengujian teknikal lainnya untuk memastikan keamanan, seperti dengan melakukan *vulnerability assessment* dan *penetration testing*.

o. Perubahan darurat (*emergency*)

Apabila terdapat perubahan yang perlu dilakukan dengan segera, perubahan darurat dapat dilakukan ke dalam sistem produksi namun dengan tetap menjalankan kontrol yang memadai.

14.2.3 Review teknikal setelah perubahan *platform*

Apabila terjadi perubahan sistem operasi, perangkat lunak bisnis perlu diuji dan ditinjau dampaknya terhadap perangkat lunak, termasuk dampak terhadap kontrol keamanan, integritas data, serta fungsi perangkat lunak.

14.2.4 Pembatasan perubahan pada *software package*

Hal-hal yang perlu diperhatikan dalam pembatasan perubahan pada *software package* sebagai berikut.

a. Perubahan *software package* yang disediakan pihak ketiga

Perubahan *software package* yang disediakan oleh pihak ketiga perlu mengikuti ketentuan berikut:

1. Mendapatkan persetujuan oleh mitra kerja.
2. Pengkajian risiko dan dampak apabila setelah melakukan perubahan, PLN akan bertanggung jawab untuk pemeliharaan perangkat lunak di masa mendatang.
3. Seluruh perubahan mengikuti proses manajemen perubahan yang berlaku.
4. Seluruh perubahan harus didokumentasikan secara memadai, sehingga perubahan tersebut dapat tetap diimplementasikan pada saat *upgrade* perangkat lunak versi berikutnya.

5. Memastikan perubahan yang dilakukan tidak dapat mengurangi efektivitas kontrol keamanan sebagaimana kondisi *software package* awal.
- b. Akses mitra kerja terhadap *software package*

Setiap *software package* dari pihak ketiga yang digunakan oleh PLN untuk sistem operasional harus bebas dari mekanisme *deactivation*, atau *destruction* yang diakibatkan oleh vendor tanpa persetujuan PLN.

14.2.5 Prinsip keamanan pengembangan sistem

Pengembangan sistem perlu mengikuti prinsip-prinsip keamanan, antara lain:

- a. Keamanan adalah bagian yang tidak terpisahkan pada saat pengembangan sistem
- b. Informasi dan data harus terlindungi secara memadai, pada saat diproses, dikirimkan, dan disimpan
- c. Asumsi bahwa sistem atau jaringan eksternal adalah tidak aman
- d. Akses terhadap sistem/ objek mengikuti prinsip *least privilege*, yaitu akses hanya diberikan kepada yang berwenang
- e. Desain, implementasi, dan interaksi sistem dengan sistem lainnya perlu didefinisikan dengan sederhana agar mudah dipahami, dianalisis, diverifikasi, dan diuji coba
- f. Pembatasan akses dengan prinsip pemberian *least privilege* dan pemisahan akses untuk menghindari *conflicting duties*
- g. Menerapkan kontrol keamanan untuk memastikan *confidentiality*, *integrity* dan *availability*

14.2.6 Keamanan lingkungan pengembangan

Hal-hal yang perlu diperhatikan dalam keamanan lingkungan pengembangan sebagai berikut.

- a. Pemisahan lingkungan pengembangan

Lingkungan pengembangan perlu dipisahkan dari lingkungan produksi atau operasional, baik terpisah secara fisik maupun *logic*.

- b. Kontrol keamanan pada lingkungan pengembangan

Lingkungan pengembangan perlu diamankan dengan kontrol pengamanan yang memadai.

- c. Pengamanan akses pada lingkungan pengembangan

Manajemen hak akses, termasuk pemberian, modifikasi, serta penghapusan akses pada lingkungan pengembangan harus melalui prosedur manajemen hak akses yang berlaku. Akses ke lingkungan pengembangan dibatasi kepada personel yang

berwenang yang telah diberi kewenangan atau otorisasi.

d. Akses pihak ketiga ke lingkungan pengembangan

Akses mitra kerja pada lingkungan pengembangan perlu mendapatkan persetujuan manajemen PLN serta dibatasi sesuai jangka waktu pekerjaan dan diawasi aktivitasnya.

e. Pencatatan perubahan di lingkungan pengembangan

Perubahan di lingkungan pengembangan harus dicatat dalam log aktivitas dan dipantau secara berkala.

f. *Backup* lingkungan pengembangan

Lingkungan pengembangan harus di-*backup* secara berkala.

g. Data rahasia di lingkungan pengembangan

PLN tidak diperkenankan menyimpan data sensitif dan rahasia pada lingkungan pengembangan.

14.2.7 Pengembangan perangkat lunak oleh mitra kerja

Pengembangan perangkat lunak oleh mitra kerja perlu memperhatikan hal-hal berikut:

a. Perangkat lunak dikembangkan oleh mitra kerja yang kompeten

Perangkat lunak harus dikembangkan oleh mitra kerja dengan reputasi yang baik serta dibuat oleh personel yang kompeten dan dapat dipercaya.

b. Perjanjian pengembangan perangkat lunak oleh mitra kerja

Mitra kerja yang mengembangkan perangkat lunak PLN harus didasari dengan kontrak yang termasuk, namun tidak terbatas pada definisi yang jelas dari perjanjian, ekspektasi akan ketepatan dan kualitas, dokumentasi perjanjian, prosedur audit, dan persyaratan pengujian.

c. Pengujian kualitas perangkat lunak yang dikembangkan mitra kerja

Perangkat lunak yang dikembangkan mitra kerja harus diuji terlebih dahulu oleh manajemen dalam memastikan kualitas dan kesesuaian perangkat lunak dengan spesifikasi yang diharapkan, termasuk pengujian atas persyaratan keamanan.

d. Pengaturan lisensi perangkat lunak yang dikembangkan mitra kerja

Dalam hal perangkat lunak dikembangkan oleh mitra kerja, PLN harus membuat kesepakatan dengan *supplier* terkait hak milik dan kepemilikan lisensi kode program yang harus disetujui bersama dan didokumentasikan.

e. Penanganan *source code* yang dikembangkan mitra kerja

Jika perangkat lunak yang dikembangkan mitra kerja digunakan untuk aktivitas bisnis yang kritikal dan *source code* tidak diberikan, mitra kerja harus menyediakan akses ke *source code* melalui perjanjian *escrow* (*escrow agreement*) dengan mitra kerja. Dalam

escrow agreement terdapat mitra kerja independen yang ditunjuk untuk menyimpan *source code*. PLN secara periodik harus memastikan bahwa mitra kerja menyimpan versi terkini dari *source code*. Agen penyimpanan yang dipilih harus memastikan nomor dan tanggal versi *source code* yang disimpan dan memastikan integritas *source code*.

14.2.8 Pengujian keamanan sistem

Sistem yang dikembangkan baik secara *in-house* atau oleh mitra kerja harus diuji untuk mengidentifikasi kerentanan dan risiko keamanan yang ada. Pengujian keamanan dilakukan secara berkala, atau apabila terdapat perubahan yang signifikan di dalam sistem. Hasil pengujian tersebut harus ditindaklanjuti dengan menanggulangi kerentanan dan risiko keamanan yang telah diidentifikasi.

14.2.9 System acceptance testing

Sistem informasi baru, *upgrade* atau yang telah dimodifikasi harus diuji coba terlebih dahulu sebelum digunakan di lingkungan produksi. Uji coba tersebut harus dilakukan dengan melibatkan pengguna sistem informasi.

14.2.10 Pengelolaan dan pemeliharaan perangkat lunak

Perangkat lunak harus dikelola dan dipelihara untuk memastikan perangkat lunak dikonfigurasi sesuai dengan kebutuhan dan standar keamanan yang berlaku, serta diverifikasi untuk mengidentifikasi adanya *error* dan kebutuhan perangkat lunak untuk *update* menggunakan versi terbaru. Hasil pengelolaan dan pemeliharaan perangkat harus didokumentasikan dan dilaporkan.

14.3 Data pengujian

14.3.1 Perlindungan data pengujian

Data untuk uji coba perlu dilindungi sebagai berikut:

- a. Kontrol akses yang sama perlu diterapkan sebagaimana lingkungan produksi.
- b. Aktivitas pemindahan data produksi ke lingkungan pengujian perlu disetujui oleh *information owner*.
- c. Data pada lingkungan pengujian perlu dilindungi sesuai dengan klasifikasinya. Data sensitif dan rahasia harus dimanipulasi atau di-*masking* (diacak, dihapus, atau diganti).

15 Kerjasama dengan mitra kerja

15.1 Keamanan dalam kerjasama mitra kerja

15.1.1 Kebijakan keamanan dalam kerjasama mitra kerja

Hal-hal yang perlu diperhatikan terkait kebijakan keamanan dalam kerjasama mitra kerja sebagai berikut:

a. Akses *logic* mitra kerja

Akses *logic* mitra kerja ke dalam lingkungan sistem PLN harus mengikuti prosedur keamanan akses *logic* yang berlaku untuk pengamanan informasi.

b. Akses fisik mitra kerja

Akses fisik *supplier* ke dalam area aman, lingkungan kerja, area aman dan fasilitas pengelolahan informasi harus mengikuti prosedur keamanan akses fisik yang berlaku untuk pengamanan informasi.

c. Kesadaran mitra kerja terhadap kebijakan keamanan data dan informasi

Kebijakan, prosedur dan tanggung jawab atas keamanan data dan informasi harus dikomunikasikan kepada *supplier* sebelum mengakses aset data dan informasi PLN, diantaranya:

1. Mitra kerja harus mematuhi segala ketentuan yang berlaku di PLN, termasuk mematuhi kebijakan dan prosedur keamanan.
2. Mitra kerja harus melindungi kerahasiaan informasi PLN.
3. Mitra kerja harus mengkomunikasikan insiden keamanan yang terjadi sehubungan dengan akses *supplier* atau aset data dan informasi PLN.
4. Mitra kerja harus mematuhi segala ketentuan keamanan data dan informasi lainnya yang telah diatur dalam perjanjian kerjasama dengan PLN.

15.1.2 Perjanjian keamanan dengan mitra kerja

Akses mitra kerja harus didasarkan pada perjanjian resmi yang memuat persyaratan keamanan secara spesifik untuk memastikan kepatuhan dengan kebijakan dan standar keamanan PLN. Perjanjian dengan *supplier* harus memuat ketentuan yang meliputi namun tidak terbatas pada:

- a. Informasi umum kepatuhan kebijakan keamanan
- b. Perjanjian tidak mengungkapkan (*non-disclosure*) informasi internal milik PLN
- c. Prosedur perlindungan aset. Aset meliputi aset fisik, informasi, dan perangkat lunak
- d. Perjanjian kontrol akses yang memaparkan metode akses yang diperbolehkan

1. PLN berhak untuk memantau dan mencabut aktivitas *user*.
2. PLN berhak untuk mengaudit tanggung jawab mitra kerja sesuai ruang lingkup perjanjian.
3. Kesepakatan atas proses eskalasi atau rencana kontingensi dalam penyelesaian masalah.
4. Struktur pelaporan yang jelas dan format pelaporan yang disepakati.
5. Mekanisme dan kontrol perlindungan fisik yang dibutuhkan untuk memastikan kepatuhan.
6. Kontrol untuk memastikan perlindungan terhadap perangkat lunak berbahaya.
7. Kesepakatan dalam pelaporan, notifikasi dan penyelidikan insiden dan pelanggaran keamanan.
8. Ketentuan untuk memastikan perlindungan dan kerahasiaan data termasuk pegawai, pelanggan, dan mitra kerja PLN.
9. Apabila ada keterlibatan mitra kerja dengan pihak lain atau subkontraktor, maka ketentuan yang ada juga berlaku untuk subkontraktor tersebut.

Klausul perjanjian harus disetujui oleh Manajemen PLN dan dimasukkan dalam semua perjanjian dengan pihak ketiga.

15.1.3 Persyaratan keamanan dalam *supply chain*

Ketentuan dan persyaratan keamanan dalam perjanjian mitra kerja harus mempertimbangkan risiko keamanan yang berkaitan dengan *supply chain* layanan dan produk IT/OT.

15.2 Manajemen mitra kerja

15.2.1 Pengawasan dan *review* layanan mitra kerja

Layanan yang diberikan oleh *supplier* harus dipantau secara rutin untuk memastikan dan menjaga kualitas layanan sesuai dengan *service level agreement* (SLA) yang ditetapkan. Evaluasi terhadap layanan juga harus dilakukan untuk mengidentifikasi ketepatan waktu dan ketepatan hasil penyampaian layanan. *Supplier* juga harus memberikan laporan atas status layanan secara rutin kepada PLN.

15.2.2 Hak audit atas mitra kerja

PLN berhak mengaudit *supplier* apabila terjadi permasalahan atau insiden signifikan selama penyampaikan layanan. Frekuensi, ruang lingkup dan tingkat kedalaman audit harus disesuaikan dengan tingkat risikonya kepada PLN. Temuan hasil audit dan rekomendasi harus didiskusikan, disetujui dan ditindaklanjuti.

15.2.3 Manajemen perubahan terhadap layanan mitra kerja

Perubahan perjanjian kerjasama dengan *supplier* harus dilakukan dengan persetujuan kedua pihak sesuai dengan prosedur perubahan yang berlaku. Pengkajian risiko harus dilakukan untuk setiap perubahan ketentuan dan persyaratan keamanan data dan informasi untuk *supplier*.

16 Keamanan data dan informasi dalam manajemen keberlangsungan bisnis

16.1 Keberlangsungan keamanan data dan informasi

16.1.1 Keamanan data dan informasi dalam *business continuity management* (BCM)

Business continuity management PLN harus mempertimbangkan dan mencakup prosedur yang diperlukan dalam menjamin keberlangsungan keamanan data dan informasi pada saat situasi darurat atau bencana.

16.1.2 *Business continuity plan* (BCP)

BCP harus dikembangkan mengacu pada kerangka kerja *best practice*, direview secara berkala, dapat diakses dan mendorong seluruh partisipasi seluruh pegawai serta menuangkan analisa dampak sebagai rencana kontingensi apabila operasional terganggu sebagai dampak dari bencana alam, kegagalan proses bisnis dan gangguan lainnya sehingga layanan dapat dikembalikan dalam durasi waktu yang telah ditentukan.

16.1.3 Implementasi keberlangsungan keamanan data dan informasi

Hal-hal yang perlu diperhatikan dalam implementasi keberlangsungan keamanan data dan informasi sebagai berikut:

a. Klasifikasi *resource* informasi

Manajemen pengoperasian komputer harus menetapkan dan menggunakan kerangka logis untuk mengklasifikasi semua sumber daya informasi dengan prioritas pemulihan pada sumber daya informasi yang paling kritis.

b. Penyiapan dan pengelolaan rencana kontingensi bisnis

Manajemen harus menyiapkan, memperbarui secara periodik, dan menguji secara berkala rencana pemulihan bisnis untuk menentukan cara dalam menyediakan fasilitas alternatif sehingga pegawai dapat melanjutkan pengoperasian ketika terjadi gangguan pada bisnis.

c. Kontrol pada keberlangsungan keamanan data dan informasi

Manajemen harus melakukan verifikasi atas kontrol keberlangsungan keamanan data dan informasi yang dikembangkan dan diimplementasikan dalam jangka waktu untuk dapat memastikan bahwa BCP tersebut masih valid dan efektif dalam situasi yang dapat merugikan.

d. Kembali ke prosedur manual

Jika aktivitas-aktivitas bisnis kritis PLN dapat dilaksanakan secara normal dengan prosedur manual dibandingkan dengan menggunakan komputer, maka suatu rencana kontingensi manual harus dikembangkan, diuji, diperbarui (*update*) secara periodik, dan diintegrasikan ke dalam rencana kontingensi komputer dan sistem komunikasi.

e. Perotasi personel *off-site*

Para pegawai *off-site* yang berpartisipasi dalam operasi pemulihan sistem informasi PLN harus dirotasi secara berkala sehingga sedikitnya ada dua orang yang memiliki pengetahuan teknis yang diperlukan untuk melaksanakan setiap pekerjaan untuk pemulihan bisnis yang utama.

f. Kebutuhan dukungan dalam keadaan darurat dan bencana

Semua Divisi yang memerlukan dukungan Divisi STI khususnya untuk keadaan darurat atau bencana harus menerapkan perangkat keras, perangkat lunak, kebijakan, dan prosedur yang berkaitan secara konsisten dengan standar PLN.

g. *Disaster recovery center* (DRC)

Lokasi DRC harus minimal mempertimbangkan antara lain:

1. DRC harus memberikan tingkat keamanan yang sama dengan lokasi utama.
2. Tingkat risiko DRC mengalami gangguan atau bencana.
3. Jarak optimal dari lokasi operasional utama.
4. Ketersediaan dan kualitas suplai listrik dan jaringan komunikasi.
5. Skalabilitas, apabila nantinya PLN membutuhkan perluasan lokasi sebagai dampak dari meningkatnya kebutuhan bisnis.
6. Ketersediaan akses mobilisasi/transportasi barang dan personel.

h. Uji coba BCP

Metode uji coba untuk memastikan BCP berjalan sesuai yang diharapkan dapat dilakukan dengan cara:

1. *Table-top testing* sesuai prosedur pemulihan (BCP).
2. Ketahanan teknis dan pengujian *disaster recovery* (untuk memastikan sistem informasi tetap beroperasi saat terjadi gangguan kecil atau sistem informasi dapat dikembalikan saat terjadi bencana).

3. Uji coba sistem dan aplikasi di lokasi pada *data center* dan *disaster recovery center* tanpa mempengaruhi operasional utama yang sedang berjalan.
4. Latihan simulasi skenario bencana tertentu.
5. Kerjasama dengan mitra kerja (apabila memungkinkan).

Hasil pengujian tersebut harus didokumentasikan dan dilaporkan kepada manajemen.

16.2 Redundansi

16.2.1 Ketersediaan fasilitas pemrosesan informasi

Ketersediaan fasilitas pemrosesan informasi perlu memperhatikan hal-hal sebagai berikut:

a. Identifikasi fasilitas pemrosesan informasi

PLN harus melakukan identifikasi terhadap sumber daya dan fasilitas pemrosesan informasi yang dimiliki dan dikelola oleh PLN maupun pihak ketiga. Untuk seluruh sumber daya dan fasilitas pemrosesan informasi yang kritikal, PLN harus merancang agar apabila terjadi kegagalan pada perangkat utama, maka terdapat perangkat cadangan lain sehingga layanan tetap dapat tersedia. Sumber daya dan fasilitas pemrosesan informasi tersebut meliputi namun tidak terbatas pada:

1. Perangkat komputer, termasuk server aplikasi dan server operasional bisnis.
2. Perangkat keamanan.
3. Media tempat penyimpanan elektronik.
4. Jaringan komunikasi.

b. Redundansi untuk fasilitas pemrosesan informasi

Fasilitas pemrosesan informasi harus diimplementasikan dengan redundansi yang cukup untuk memenuhi kebutuhan ketersediaan, seperti:

1. *Business continuity manager* harus memastikan bahwa BCP telah terkoordinasi secara menyeluruh di dalam PLN sehingga tidak terdapat konflik yang mungkin terjadi dengan rencana *emergency* lainnya yang akan diinisiasi ketika terjadi suatu insiden atau bencana.
2. Suplai listrik dan jaringan komunikasi atau internet harus dijamin ketersediaannya dengan menggunakan lebih dari 1 penyedia layanan.
3. Jaringan komputer dirancang untuk mencegah adanya *single point of failure*.
4. Penggunaan UPS untuk perangkat komputer.
5. Penggunaan perangkat primer dan perangkat sekunder yang dikonfigurasi untuk melakukan *fail-over* baik secara otomatis atau manual apabila salah satu perangkat mengalami kegagalan.
6. Kapasitas perangkat komputer dan media harus disesuaikan dengan kebutuhan untuk mencegah kegagalan.

17 Kepatuhan

17.1 Audit keamanan data dan informasi

17.1.1 Audit independen terhadap keamanan data dan informasi

Hal-hal yang perlu diperhatikan dalam audit independen terhadap keamanan data dan informasi sebagai berikut.

- a. Review keamanan data dan informasi oleh pihak independen

Review oleh pihak independen harus dilakukan untuk melakukan evaluasi terhadap implementasi kontrol keamanan data dan informasi dalam memastikan kesesuaian, kecukupan, dan efektivitas kontrol keamanan yang telah diterapkan. Review harus dilakukan secara independen oleh audit internal, manajemen yang independen, atau pihak ketiga/eksternal.

- b. Pelaporan hasil review keamanan data dan informasi

Hasil review keamanan data dan informasi harus didokumentasikan dan dilaporkan kepada manajemen PLN.

17.1.2 Kepatuhan dengan kebijakan dan standar keamanan

Hal-hal yang perlu diperhatikan dalam kepatuhan dengan kebijakan dan standar keamanan sebagai berikut:

- a. Rencana untuk kepatuhan keamanan data dan informasi

Manajemen PLN harus menyiapkan rencana tahunan untuk memastikan kepatuhan sistem komputer dan komunikasi terhadap kebijakan dan standar yang telah ditetapkan.

- b. Standar implementasi kontrol

Manajemen harus mengimplementasikan kontrol keamanan data dan informasi secara konsisten dengan praktik bisnis umumnya dan konsisten dengan tingkat kritis, nilai, dan sensitivitas informasi yang dikelola.

- c. Penilaian risiko sistem

Setiap unit organisasi PLN yang mengelola komputer dan jaringannya sendiri harus melakukan pemeriksaan yang berkenaan dengan keamanan data dan informasi (*security-related risk assessment*) sistem tersebut, dan memastikan bahwa tindakan keamanan data dan informasi yang memadai telah dilakukan.

17.1.3 Review kepatuhan

Semua ketentuan terkait kepatuhan hukum, regulasi dan hak kekayaan intelektual mengikuti ketentuan yang berlaku.

Hal-hal yang perlu diperhatikan terkait kepatuhan teknis sebagai berikut:

- a. Kepatuhan teknis perangkat keras dan perangkat lunak

Penggunaan perangkat lunak dan perangkat keras dalam mendukung bisnis organisasi harus mematuhi kebijakan keamanan teknis.

- b. Audit *backup* lingkungan produksi

Audit internal harus melakukan *review* tahunan rutin dan melakukan pengujian secara acak terhadap proses *backup* sistem komputer untuk kegiatan bisnis.

- c. Pemeriksaan keamanan terhadap risiko sistem informasi

Pemeriksaan risiko keamanan data dan informasi untuk sistem informasi kritis dan aplikasi produksi kritis harus dilaksanakan sedikitnya sekali dalam dua tahun, dan semua *upgrade* perbaikan utama, konversi, dan semua perubahan yang berhubungan dengan sistem dan aplikasi tersebut harus didahului oleh penilaian risiko.

- d. Pemeriksaan risiko keamanan data dan informasi dalam organisasi (*organization-wide information security risk assessment*)

Setiap tahun manajemen PLN harus melakukan tindakan atau mengelola pihak independen yang melakukan tindakan pemeriksaan risiko untuk seluruh perusahaan (*enterprise-wide risk assessment*) dan menghasilkan laporan dari proyek yang didalamnya berisi deskripsi rinci risiko keamanan data dan informasi yang sedang dihadapai oleh organisasi serta rekomendasi spesifik untuk mencegah atau memitigasi risiko-risiko tersebut.

- e. Ahli evaluasi sistem keamanan

Evaluasi, audit, analisis dan uji coba atas kerentanan keamanan sistem informasi harus dilakukan oleh personel ahli yang berkompeten, terpercaya, dan independen dibawah supervisi organisasi penanggung jawab keamanan data dan informasi.

- f. *Tools* audit keamanan sistem

Apabila dalam proses *review* teknikal menggunakan *tools*, maka pengendalian dan kontrol yang sesuai perlu diterapkan untuk menghindari gangguan teknis dan penyalahgunaan *tools* yang dapat menimbulkan gangguan pada sistem.

- g. Hasil *review* keamanan teknikal

Apabila terdapat isu dan kerentanan yang dideteksi pada saat *review* keamanan teknikal, maka perlu ditindaklanjuti dengan perbaikan atau proses manajemen dan pengendalian risiko yang memadai. Isu dan kerentanan tersebut perlu dimonitor secara rutin hingga seluruhnya telah selesai ditindaklanjuti.

17.1.4 Pengamanan data rekaman

Hal-hal yang perlu diperhatikan dalam pengamanan data rekaman sebagai berikut.

- a. Kebijakan dalam manajemen pengamanan data rekaman

Kebijakan manajemen informasi elektronik harus dilindungi secara memadai, antara lain:

1. Manajemen harus mengeluarkan prosedur terkait jangka waktu retensi, penyimpanan, penanganan dan pemusnahan data rekaman dan informasi. Prosedur tersebut setidaknya harus mencakup proses penanganan dokumen e-mail, kebijakan teknikal manajemen informasi, kepemilikan informasi, serta kewajiban untuk memelihara keamanan data dan informasi.
2. Jangka waktu retensi harus ditetapkan untuk mengidentifikasi data rekaman yang harus terpelihara berdasarkan periode waktu yang telah ditetapkan.

- b. Retensi informasi sensitif

Masa retensi harus ditentukan pada semua informasi yang sensitif.

- c. Identifikasi catatan penting (*vital record*)

Manajer divisi harus mengidentifikasi dan mengelola daftar catatan penting terbaru, yang dibutuhkan jika terjadi bencana untuk disimpan di divisinya.

- d. Penyimpanan catatan penting

Catatan bisnis penting harus tersimpan dalam penyimpanan terkunci dan tahan api jika tidak sedang digunakan untuk kegiatan bisnis.

- e. Jadwal penjagaan sumber data

Semua informasi PLN harus dijaga (*retained*) secara aman sesuai jadwal yang dibuat oleh Manajemen PLN.

- f. Penyimpanan dokumen sumber bisnis

Dokumen-dokumen sumber dan *file* masukan elektronik asli harus disimpan sampai transaksi terkait telah selesai, *review* manajemen memasukkan dari catatan-catatan transaksi digabungkan dengan transaksi-transaksi ini telah dilakukan dan periode dimana transaksi-transaksi dapat menjadi sengketa telah berlalu.

- g. Penyimpanan data transaksi aplikasi

Semua data transaksi aplikasi harus dikelola dalam tempat yang terlindung atau terproteksi hingga seluruh *backup* dari dari semua *master file* kegiatan bisnis yang terkait telah diselesaikan.

- h. Pemusnahan informasi

Semua informasi perusahaan harus dimusnahkan atau dibuang jika tidak lagi diperlukan.

i. Penyimpanan informasi sensitif untuk penghancuran

Pegawai tidak boleh menaruh/membuang dokumen informasi yang sensitif di tempat pembuangan sampah publik dan harus menjaga serta mengawasi informasi yang sensitif hingga dapat dimusnahkan dengan metode yang sesuai.

j. Penyimpanan informasi pelanggaran dan masalah keamanan

Informasi yang menjelaskan semua masalah dan pelanggaran keamanan data dan informasi yang telah dilaporkan harus dijaga selama jangka waktu sesuai ketentuan perusahaan.

Pengelola Standardisasi:

PT PLN (Persero) Pusat Penelitian dan Pengembangan Ketenagalistrikan

Jl. Duren Tiga Raya No. 102, Jakarta 12760, Telp. 021-7973774

www.pln.co.id

Pengelola Standardisasi:

PT PLN (Persero) Pusat Penelitian dan Pengembangan Ketenagalistrikan
Jl. Duren Tiga Raya No. 102, Jakarta 12760, Telp. 021-7973774
www.pln.co.id