MENTERI PELINDUNGAN PEKERJA MIGRAN INDONESIA/
KEPALA BADAN PELINDUNGAN PEKERJA MIGRAN INDONESIA
REPUBLIK INDONESIA

KEPUTUSAN MENTERI PELINDUNGAN PEKERJA MIGRAN INDONESIA/
KEPALA BADAN PELINDUNGAN PEKERJA MIGRAN INDONESIA
REPUBLIK INDONESIA
NOMOR 837 TAHUN 2026
TENTANG
PEDOMAN PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK
KEMENTERIAN PELINDUNGAN PEKERJA MIGRAN INDONESIA/
BADAN PELINDUNGAN PEKERJA MIGRAN INDONESIA

MENTERI PELINDUNGAN PEKERJA MIGRAN INDONESIA/
KEPALA BADAN PELINDUNGAN PEKERJA MIGRAN INDONESIA
REPUBLIK INDONESIA,

Menimbang : a. bahwa dalam rangka melindungi kerahasiaan (*confidentiality*), keutuhan (*integrity*), ketersediaan (*availability*), keaslian (*authentication*), dan kenirsangkalan (*nonrepudiation*) aset informasi Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia dari berbagai bentuk ancaman keamanan informasi,baik dari dalam maupun dari luar lingkungan Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia, perlu melakukan pengelolaan keamanan informasi di Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia;

b. bahwa dalam rangka pengelolaan keamanan informasi di lingkungan Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia, perlu menyusun kebijakan dan standar sistem manajemen keamanan informasi;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Keputusan Menteri Pelindungan Pekerja Migran Indonesia/Kepala Badan Pelindungan Pekerja Migran Indonesia tentang Pedoman Penerapan Sistem Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia;

Mengingat : 1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952;

2. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);

3. Undang-Undang Nomor 18 Tahun 2017 tentang Pelindungan Pekerja Migran Indonesia (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 242, Tambahan Lembaran Negara Republik Indonesia Nomor 6141) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja Menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);

4. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);

5. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

6. Peraturan Presiden Nomor 132 Tahun 2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 233)

7. Peraturan Presiden Nomor 165 Tahun 2024 tentang Kementerian Pelindungan Pekerja Migran Indonesia (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 361);

8. Peraturan Presiden Nomor 166 Tahun 2024 tentang Badan Pelindungan Pekerja Migran Indonesia (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 362);

9. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);
10. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
11. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber (Berita Negara Republik Indonesia Tahun 2024 Nomor 43);
12. Peraturan Menteri Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia Nomor 1 Tahun 2024 tentang Organisasi dan Tata Kerja Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia (Berita Negara Republik Indonesia Tahun 2024 Nomor 975) sebagaimana telah diubah dengan Peraturan Menteri Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia Nomor 6 Tahun 2026 tentang Perubahan Atas Peraturan Menteri Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia Nomor 1 Tahun 2024 tentang Organisasi dan Tata Kerja Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia (Berita Negara Republik Indonesia Tahun 2026 Nomor 447);
13. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2024 tentang Standar dan Tata Cara Pelaksanaan Audit Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2024 Nomor 655);
14. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 8 Tahun 2026 tentang Evaluasi Kinerja dan Reformasi Birokrasi (Berita Negara Repbulik Indonesia Tahun 2026 Nomor 364);
15. Peraturan Menteri Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia Nomor 8 Tahun 2026 tentang Satu Data Bidang Pelindungan Pekerja Migran Indonesia (Berita Negara Republik Indonesia Tahun 2026 Nomor 527);

MEMUTUSKAN:

Menetapkan : KEPUTUSAN MENTERI PELINDUNGAN PEKERJA MIGRAN INDONESIA/KEPALA BADAN PELINDUNGAN PEKERJA MIGRAN INDONESIA TENTANG PEDOMAN PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK KEMENTERIAN PELINDUNGAN PEKERJA MIGRAN INDONESIA/BADAN PELINDUNGAN PEKERJA MIGRAN INDONESIA.

KESATU : Menetapkan Pedoman Penerapan Sistem Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia, yang selanjutnya disebut Sistem Manajemen Keamanan Informasi, sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Keputusan Menteri/Kepala Badan ini.

KEDUA : Sistem Manajemen Keamanan Informasi sebagaimana dimaksud dalam Diktum KESATU menjadi acuan atau standar dalam rangka melindungi aset informasi Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia dari berbagai bentuk ancaman baik dari dalam maupun dari luar lingkungan Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia, dengan tujuan untuk menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi.

KETIGA : Sistem Manajemen Keamanan Informasi sebagaimana dimaksud dalam Diktum KEDUA terdiri atas:

a. organisasi keamanan informasi;
b. perencanaan keamanan informasi;
c. dukungan pengoperasian;
d. keamanan sumber daya manusia;
e. keamanan aset;
f. keamanan akses;
g. keamanan kriptografi;
h. keamanan fisik dan lingkungan;
i. keamanan operasional;
j. keamanan komunikasi;
k. keamanan pengembangan dan pemeliharaan;
l. keamanan pihak ketiga;
m. manajemen insiden siber;
n. manajemen keberlangsungan layanan informasi;
o. pengendalian kepatuhan;
p. audit keamanan informasi; dan
q. evaluasi kinerja dan perbaikan berkelanjutan keamanan informasi.

KEEMPAT : Kepala Pusat Data dan Informasi selaku pengelola teknis operasional keamanan informasi berwenang menetapkan standar teknis, pedoman operasional, dan prosedur pengamanan infrastruktur, aplikasi, serta aset informasi yang berlaku di lingkungan Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia.

KELIMA : Pada saat Keputusan Menteri/Kepala Badan ini berlaku, Keputusan Badan Pelindungan Pekerja Migran Indonesia Nomor 501 Tahun 2023 tentang Sistem Manajemen Keamanan Informasi Badan Pelindungan Pekerja Migran Indonesia dicabut dan dinyatakan tidak berlaku.

KEENAM : Keputusan Menteri/Kepala Badan ini mulai berlaku pada sejak tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 04 Mei 2026
MENTERI PELINDUNGAN
PEKERJA MIGRAN INDONESIA/
KEPALA BADAN PELINDUNGAN
PEKERJA MIGRAN INDONESIA
REPUBLIK INDONESIA,

MUKHTARUDIN

LAMPIRAN
KEPUTUSAN MENTERI PELINDUNGAN PEKERJA MIGRAN INDONESIA/ KEPALA BADAN PELINDUNGAN PEKERJA MIGRAN INDONESIA
REPUBLIK INDONESIA
NOMOR 837 TAHUN 2026
TENTANG PEDOMAN PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK KEMENTERIAN PELINDUNGAN PEKERJA MIGRAN INDONESIA/BADAN PELINDUNGAN PEKERJA MIGRAN INDONESIA

PEDOMAN PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK KEMENTERIAN PELINDUNGAN PEKERJA MIGRAN INDONESIA/ BADAN PELINDUNGAN PEKERJA MIGRAN INDONESIA

BAB I
PENDAHULUAN

A. Latar belakang

Berdasarkan Peraturan Presiden Nomor 165 Tahun 2024 tentang Kementerian Pelindungan Pekerja Migran Indonesia, telah terjadi transformasi kelembagaan dari Badan Pelindungan Pekerja Migran Indonesia menjadi Kementerian Pelindungan Pekerja Migran Indonesia. Dalam menjalankan tugas menyelenggarakan suburusan pemerintahan pelindungan Pekerja Migran Indonesia yang merupakan lingkup pemerintahan di bidang ketenagakerjaan untuk membantu Presiden dalam menyelenggarakan pemerintahan negara. Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia mengumpulkan, menyimpan, dan mengelola informasi dalam skala besar yang bersifat sensitif dan memiliki risiko tinggi. Data tersebut mencakup informasi identitas pribadi, informasi penempatan, hingga data pengaduan Pekerja Migran Indonesia, dan data terkait lainnya.

Seiring dengan peningkatan implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE), Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia dihadapkan pada berbagai tantangan keamanan informasi internal yang memerlukan penanganan komprehensif. Salah satu tantangan utama adalah tingkat kesadaran keamanan informasi (*security awareness*) aparatur yang masih perlu ditingkatkan guna memitigasi risiko kelalaian operasional. Kondisi tersebut diperparah oleh temuan berdasarkan pemantauan ancaman siber, yang mengindikasikan adanya kebocoran kredensial akun pegawai pada situs gelap (*dark web*) sehingga berpotensi mengancam kerahasiaan dan integritas data instansi.

Dari tinjauan aspek teknis dan operasional, siklus pengembangan aplikasi di lingkungan Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia belum sepenuhnya mengimplementasikan prinsip keamanan sejak tahap perancangan (*security by design*). Hal tersebut tercermin dari belum diterapkannya pengujian kerentanan dan penetrasi (*Vulnerability Assessment and Penetration Testing*/VAPT) secara menyeluruh dan terstandar pada seluruh aplikasi, baik sistem yang telah beroperasi, sistem dalam tahap pengembangan, maupun pada penambahan modul baru. Kompleksitas kerentanan sistem informasi ini menimbulkan risiko siber yang tinggi, khususnya ketika dihadapkan pada keterbatasan kapasitas dan kuantitas Sumber Daya Manusia (SDM) teknis yang memiliki kompetensi spesifik untuk merespons serta menangani insiden keamanan siber.

Dari sisi eksternal, tren ancaman siber global yang semakin kompleks, seperti *ransomware*, *malware*, *Distributed Denial of Service* (DDoS), dan peretasan menjadi ancaman nyata yang dapat mengakibatkan kerugian finansial dan hilangnya kepercayaan masyarakat. Menghadapi ancaman tersebut, Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia belum secara optimal memiliki pedoman keberlangsungan dan pemulihan layanan yang komprehensif, seperti Dokumen Perencanaan Keberlangsungan Bisnis (*Business Continuity Plan*/BCP), Pemulihan Bencana (*Disaster Recovery Plan*/DRP), dan Rencana Tanggap Insiden (*Incident Response Plan*/IRP). Lebih lanjut, sejalan dengan disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (PDP), tata kelola dan kepatuhan pelindungan data pribadi di lingkungan KP2MI/BP2MI belum diterapkan secara maksimal, sehingga memunculkan potensi risiko hukum.

Merespons transisi kelembagaan serta tingginya kompleksitas isu internal dan eksternal tersebut, diperlukan sebuah payung kebijakan Sistem Manajemen Keamanan Informasi yang kokoh. Kebijakan Sistem Manajemen Keamanan Informasi ini disusun sebagai acuan utama dalam mengorkestrasi pengendalian keamanan untuk memberikan pelindungan kerahasiaan (*confidentiality*), keutuhan (*integrity*), ketersediaan (*availability*), keaslian (*authentication*), dan kenirsangkalan (*non-repudiation*) terhadap seluruh aset informasi Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia. Penyelenggaraan Sistem Manajemen Keamanan Informasi ini menjadi langkah strategis untuk memitigasi risiko siber, menjamin keberlangsungan layanan, serta memastikan kepatuhan organisasi terhadap peraturan perundang-undangan yang berlaku.

B. Tujuan

Kebijakan Sistem Manajemen Keamanan Informasi ini digunakan sebagai pedoman dalam rangka melindungi aset informasi Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia dari berbagai bentuk ancaman baik internal maupun eksternal, yang dilakukan secara sengaja maupun tidak sengaja. Pengamanan dan perlindungan ini diberikan untuk menjamin kerahasiaan (*confidentiality*), keutuhan (*integrity*), ketersediaan (*availability*), keaslian (*authentication*), dan kenirsangkalan (*non-repudiation*) aset informasi selalu terjaga dan terpelihara dengan baik.

C. Ruang Lingkup

Kebijakan dan standar ini berlaku untuk pengelolaan pengamanan seluruh aset informasi KP2MI/BP2MI yang dilaksanakan oleh sumber daya manusia yang terlibat baik sebagai pengguna atau pengelola, instansi pemerintah terkait, mitra kerja, dan pihak ketiga di KP2MI/BP2MI. Cakupan aset informasi meliputi data dan informasi SPBE, aplikasi SPBE, infrastruktur SPBE dan sumber daya manusia SPBE. Adapun cakupan pengaturan keamanan dalam kebijakan ini terdiri atas:

1. organisasi keamanan informasi;
2. perencanaan keamanan informasi;
3. dukungan pengoperasian;
4. keamanan sumber daya manusia;
5. keamanan aset;
6. keamanan akses;
7. keamanan kriptografi;
8. keamanan fisik dan lingkungan;
9. keamanan operasional;
10. keamanan komunikasi;
11. keamanan pengembangan dan pemeliharaan;
12. keamanan pihak ketiga;
13. manajemen insiden siber;
14. manajemen keberlangsungan layanan informasi;
15. pengendalian kepatuhan;
16. audit keamanan informasi; dan
17. evaluasi kinerja dan perbaikan berkelanjutan keamanan informasi.

D. Pengertian

Dalam pedoman ini yang dimaksud dengan:

1. Teknologi Informasi dan Komunikasi selanjutnya disebut TIK adalah terminologi yang mencakup seluruh peralatan teknis untuk memproses dan menyampaikan informasi.
2. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik
3. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
4. Data adalah tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, teleacopy atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi.
5. Informasi adalah satu atau sekumpulan Data, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *Electronic Data Interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi.
6. Aplikasi adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi layanan.

7. Infrastruktur adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat elektronik lainnya.
8. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah sistem manajemen untuk membangun, mengimplementasikan, mengoperasikan, memonitor, meninjau, memelihara dan meningkatkan keamanan informasi berdasarkan pendekatan risiko.
9. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan informasi.
10. Risiko adalah segala kejadian dalam setiap aktivitas yang mungkin timbul karena faktor ketidakpastian, yang mengandung potensi untuk menghambat pencapaian sasaran kinerja dari layanan Sistem Elektronik.
11. Manajemen Risiko adalah aktivitas terkoordinasi untuk identifikasi, penilaian, dan penentuan prioritas Risiko yang kemudian akan dikelola, dipantau, dan dikontrol untuk mengurangi dampak dan/ atau kemungkinan terjadinya Risiko tersebut.
12. Rencana Tindak Lanjut Risiko yang selanjutnya disebut RTL adalah respon yang direncanakan manajemen untuk menindaklanjuti hasil evaluasi risiko, seperti *mitigate/reduce*, *avoid*, *share/ transfer* atau *accept*.
13. Audit Teknologi Informasi dan Komunikasi yang selanjutnya disebut Audit TIK adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset teknologi informasi dan komunikasi dengan tujuan untuk menetapkan tingkat kesesuaian antara teknologi informasi dan komunikasi dengan kriteria dan/atau standar yang telah ditetapkan.
14. Audit Keamanan Informasi adalah Audit TIK cakupan keamanan informasi.
15. Auditor Keamanan Informasi adalah orang yang memiliki kompetensi untuk melakukan Audit Keamanan Informasi.
16. Kementerian Pelindungan Pekerja Migran Indonesia yang selanjutnya disebut KP2MI adalah kementerian yang menyelenggarakan suburusan pemerintahan pelindungan Pekerja Migran Indonesia yang merupakan lingkup dari urusan pemerintahan di bidang ketenagakerjaan.
17. Badan Pelindungan Pekerja Migran Indonesia yang selanjutnya disebut BP2MI adalah lembaga pemerintah nonkementerian yang melaksanakan tugas pemerintahan di bidang pelindungan Pekerja Migran Indonesia.
18. Audit Internal Keamanan Informasi adalah Audit Keamanan Informasi yang dilaksanakan oleh Auditor Keamanan Informasi internal KP2MI/BP2MI.
19. Audit Eksternal Keamanan Informasi adalah Audit Keamanan Informasi yang dilaksanakan oleh Auditor Keamanan Informasi eksternal KP2MI/BP2MI yang memiliki sertifikasi sebagai Auditor Keamanan Informasi.
20. Lembaga Pelaksana Audit TIK yang selanjutnya disebut LATIK adalah lembaga yang melaksanakan Audit Teknologi Informasi dan Komunikasi.

21. LATIK Terakreditasi yang Terdaftar adalah badan hukum yang telah terakreditasi sebagai pelaksana Audit TIK dan terdaftar pada Badan Siber dan Sandi Negara.
22. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik.
23. Insiden siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam keamanan informasi antara lain namun tidak terbatas pada *web defacement, malware* (*virus, worm, trojan backdoor dan ransomware*), *unauthorized access, data breach,* dan *Distributed Denial of Service* (DDoS).
24. Tim Tanggap Insiden Siber adalah sekelompok orang yang bertanggung jawab menangani Insiden Siber dalam ruang lingkup yang ditentukan terhadapnya.
25. Tim Pengelola Sistem Manajemen Keamanan Informasi yang selanjutnya disebut Tim SMKI adalah sekelompok orang yang bertanggung jawab untuk menyusun, mengkomunikasikan, memastikan, dan memantau pelaksanaan SMKI di KP2MI/BP2MI.
26. Pemilik Proses Bisnis adalah pimpinan unit organisasi di lingkungan Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia yang memiliki tugas, wewenang, dan tanggung jawab atas penyelenggaraan proses bisnis, serta memanfaatkan Sistem Elektronik (SE) untuk mendukung pelaksanaan tugas dan fungsi di unit kerjanya.

E. Standar Acuan

Standar yang digunakan sebagai acuan dalam pembuatan pedoman SMKI ini adalah:

1. SNI ISO/IEC 27001 – Keamanan informasi, keamanan siber, dan proteksi privasi – Sistem manajemen keamanan informasi – Persyaratan; dan
2. SNI ISO/IEC 27002 – Keamanan informasi, keamanan siber, dan proteksi privasi – Kontrol keamanan informasi.

BAB II
ORGANISASI KEAMANAN INFORMASI

A. Umum

KP2MI/BP2MI menetapkan, menerapkan, memelihara, dan memperbaiki secara berkelanjutan SMKI. SMKI dijalankan melalui organisasi keamanan informasi yang peran dan tanggung jawabnya ditetapkan melalui pedoman ini.

B. Peran

Organisasi Keamanan Informasi dalam menjalankan kegiatannya mempunyai peran masing-masing, terdiri atas:

1. Sekretaris Jenderal berperan sebagai Ketua Koordinator SPBE, selaku penanggung jawab SMKI;
2. Ketua Koordinator SPBE dalam menjalankan tugasnya sebagai penanggung jawab SMKI dibantu oleh Tim SMKI selaku pelaksana teknis keamanan informasi;
3. Tim SMKI ditetapkan oleh Ketua Koordinator SPBE;
4. Kepala Pusat Data dan Informasi berperan sebagai Ketua Tim SMKI dan mengkoordinasikan pelaksanaan manajemen keamanan informasi di lingkungan Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia;
5. Ketua Tim SMKI memiliki kewenangan dalam menentukan komposisi, kualifikasi, dan jumlah anggota Tim SMKI sesuai dengan kebutuhan operasional;
6. Inspektur Jenderal berperan sebagai pengawas internal yang melaksanakan Audit Internal Keamanan Informasi;
7. Staf Ahli Bidang Transformasi Digital berperan sebagai Penasihat yang memberikan arahan strategis, pertimbangan kebijakan, dan memastikan keselarasan penyelenggaraan keamanan informasi dengan visi transformasi digital nasional serta misi organisasi Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia; dan
8. Pejabat Pimpinan Tinggi Madya dan Pejabat Pimpinan Tinggi Pratama di lingkungan KP2MI/BP2MI sesuai kewenangan operasional unit kerjanya masing-masing sebagai Pemilik Proses Bisnis berperan dan bertanggung jawab dalam memastikan kepatuhan dan penerapan kebijakan SMKI pada operasional proses bisnis dan Sistem Elektronik di lingkungan unit kerjanya masing-masing.

C. Tanggung Jawab

1. Sekretaris Jenderal bertanggung jawab untuk:
   a) memastikan dan mengoordinasikan pelaksanaan Kebijakan SMKI di seluruh unit kerja;
   b) menyediakan sumber daya yang memadai untuk menetapkan, mengimplementasikan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan SMKI KP2MI/BP2MI;
   c) menetapkan kriteria penerimaan risiko dan tingkat risiko yang dapat diterima;
   d) memastikan terlaksananya Audit Internal Keamanan Informasi secara berkala;
   e) menyetujui dan menetapkan penunjukan pihak ketiga yang berkompeten sebagai Auditor Eksternal Keamanan Informasi;
   f) menetapkan arsitektur keamanan informasi;

g) menetapkan peta rencana 5 (lima) tahunan dan sasaran keamanan informasi setiap tahunnya;
h) melakukan tinjauan secara berkala atas pelaksanaan kebijakan SMKI; dan
i) menyampaikan kinerja pelaksanaan kebijakan SMKI kepada Menteri Pelindungan Pekerja Migran Indonesia/Kepala Badan Pelindungan Pekerja Migran Indonesia.

2. Tim SMKI bertanggung jawab untuk:
   a) menyusun, mengomunikasikan, dan memantau pelaksanaan kebijakan SMKI di KP2MI/BP2MI;
   b) melakukan analisis kebutuhan keamanan informasi, yang mencakup:
      1) mengidentifikasi Aplikasi dan Infrastruktur untuk Keamanan Informasi;
      2) mengidentifikasi standar kompetensi SDM Keamanan Informasi; dan
      3) mengidentifikasi program peningkatan kompetensi Keamanan Informasi dan penanggulangan Insiden Siber;
   c) merumuskan, mengkoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan Informasi;
   d) memastikan seluruh pembangunan/pengembangan Sistem Elektronik termasuk yang dilakukan oleh Pihak Ketiga, minimal memenuhi Standar Teknis dan Prosedur Keamanan Informasi yang ditetapkan oleh Lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber;
   e) memastikan peningkatan kesadaran, kepedulian, dan kepatuhan oleh seluruh pegawai terhadap kebijakan, prosedur, dan standar keamanan informasi;
   f) memastikan diterapkannya perjanjian menjaga kerahasiaan aset informasi yang dituangkan dalam dokumen perjanjian kerahasiaan (*Non Disclosure Agreement*);
   g) mengendalikan dan menjaga kemutakhiran kebijakan, prosedur, dan standar Keamanan Informasi;
   h) memfasilitasi pelaksanaan Audit Internal dan Audit Eksternal Keamanan Informasi;
   i) melaksanakan pengujian kerentanan dan keamanan (VAPT) secara mandiri atau melibatkan pihak ketiga yang berkompeten sebagai bagian dari evaluasi teknis;
   j) mengelola penanganan gangguan dan Insiden Siber secara terpusat melalui Tim Tanggap Insiden Siber (*Computer Security Incident Response Team*/CSIRT) KP2MI/BP2MI;
   k) memastikan diterapkannya Manajemen Risiko, Manajemen Insiden Siber, dan Manajemen Aset dalam pelaksanaan pengamanan aset Informasi;
   l) melaksanakan perbaikan penerapan Keamanan Informasi berdasarkan hasil temuan audit internal dan audit eksternal; dan
   m) menyusun laporan evaluasi penerapan Kebijakan SMKI dan menyampaikannya kepada Sekretaris Jenderal.

3. Inspektur Jenderal bertanggung jawab untuk:
   a) menyusun pedoman teknis pengawasan dan Audit Internal Keamanan Informasi;
   b) menyusun perencanaan dan memasukkan Audit Internal Keamanan Informasi ke dalam Program Kerja Pengawasan Tahunan (PKPT);

c) melaksanakan kegiatan Audit Internal Keamanan Informasi secara objektif dan independen;
d) memberikan saran, evaluasi, dan rekomendasi perbaikan atas hasil temuan Audit Internal Keamanan Informasi;
e) menyusun Laporan Hasil Audit Internal Keamanan Informasi; dan
f) menyampaikan Laporan Hasil Audit Internal Keamanan Informasi kepada Sekretaris Jenderal.

4. Staf Ahli Bidang Transformasi Digital bertanggung jawab untuk:
a) memberikan arahan strategis kepada Penanggung Jawab terkait arah kebijakan keamanan informasi agar selaras dengan rencana transformasi digital Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia;
b) memberikan pertimbangan dan masukan dalam penyusunan peta rencana (*roadmap*) jangka panjang keamanan informasi serta arsitektur keamanan informasi;
c) memastikan bahwa seluruh inisiatif keamanan informasi tetap mendukung pencapaian indikator kinerja utama (IKU) transformasi digital dan Sistem Pemerintahan Berbasis Elektronik (SPBE);
d) memberikan arahan dalam menyikapi isu-isu strategis atau ancaman keamanan siber yang berdampak pada reputasi dan keberlangsungan operasional organisasi;
e) mendorong integrasi budaya keamanan informasi ke dalam setiap aspek transformasi digital di seluruh unit kerja; dan
f) meninjau efektivitas arah kebijakan keamanan informasi berdasarkan laporan berkala dari Tim SMKI sebagai bahan masukan untuk Pembina.

5. Pemilik Proses Bisnis bertanggung jawab untuk:
a) memastikan kepatuhan seluruh pegawai di unit kerjanya terhadap kebijakan, pedoman, dan prosedur teknis SMKI yang ditetapkan;
b) melaksanakan penerapan kebijakan dan standar SMKI dalam penyelenggaraan Sistem Elektronik di lingkungan unit kerjanya;
c) mengidentifikasi klasifikasi aset informasi dan tingkat kerahasiaan data yang dikelola dalam proses bisnis unitnya;
d) memastikan hak akses terhadap Sistem Elektronik bagi pegawai di unit kerjanya diberikan, diubah, atau dicabut sesuai dengan prinsip kebutuhan pekerjaan (*need-to-know basis*);
e) melaporkan setiap dugaan pelanggaran keamanan informasi atau insiden siber yang terjadi di unit kerjanya kepada Tim SMKI;
f) berkoordinasi dengan Pusat Data dan Informasi KP2MI/BP2MI selaku Tim SMKI dalam hal penerapan kebijakan dan standar keamanan, serta penanganan gangguan keamanan informasi di wilayah kerjanya; dan
g) memberi masukan dan evaluasi terkait peningkatan efektivitas kebijakan serta standar SMKI di lingkungan KP2MI/BP2MI.

6. Koordinasi dan Tanggung Jawab Antar-Unit
a) Pusat Data dan Informasi selaku Tim SMKI bertindak sebagai koordinator teknis keamanan informasi dan bertanggung jawab menyediakan infrastruktur keamanan secara terpusat di lingkungan KP2MI/BP2MI;
b) Pejabat Pimpinan Tinggi Madya dan Pejabat Pimpinan Tinggi Pratama dapat menunjuk pengelola atau tim keamanan informasi di lingkungan unit kerjanya dengan tetap berkoordinasi dan mematuhi standar teknis yang ditetapkan oleh Pusat Data dan Informasi; dan

c) setiap pedoman, standar, atau prosedur operasional spesifik yang disusun oleh unit kerja tidak boleh bertentangan dengan kebijakan dan standar teknis keamanan informasi yang ditetapkan oleh Kepala Pusat Data dan Informasi.

BAB III
PERENCANAAN KEAMANAN INFORMASI

A. Kategorisasi Sistem Elektronik

KP2MI/BP2MI sebagai Penyelenggara SPBE untuk Sistem Elektronik Lingkup Publik, wajib melakukan kategorisasi terhadap setiap Sistem Elektronik yang dikelola sebagai salah satu dasar dalam pelaksanaan Keamanan Informasi. Penentuan Kategorisasi Sistem Elektronik dilaksanakan sesuai dengan peraturan perundang-undangan yang ditetapkan oleh Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

B. Manajemen Risiko

Pelaksanaan Keamanan Informasi diselenggarakan dengan mempertimbangkan berbagai Risiko yang dapat mengakibatkan terjadinya kegagalan pelindungan informasi di KP2MI/BP2MI. Oleh karena itu, dalam merencanakan Keamanan Informasi, Tim SMKI wajib menyelenggarakan Manajemen Risiko Keamanan Informasi, yang meliputi tahapan:

1. menyusun penilaian Risiko Keamanan Informasi dengan mengidentifikasi ancaman, kerentanan, kemungkinan (*likelihood*), dan dampak apabila Risiko tersebut terjadi;
2. menyusun Rencana Tindak Lanjut (RTL) penanganan Risiko bersama dengan Pemilik Proses Bisnis terkait; dan
3. melakukan sosialisasi dan komunikasi RTL pada para pemilik Risiko.

Proses Manajemen Risiko dilakukan secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun dan jika ada perubahan aset atau proses bisnis yang berdampak signifikan terhadap profil Risiko yang ditetapkan.

C. Perencanaan Keamanan Informasi

Tim SMKI menyusun program kerja Keamanan Informasi berdasarkan RTL sebagai wujud realisasi atas tindak lanjut Risiko Keamanan Informasi. Program kerja Keamanan Informasi paling sedikit meliputi:

1. edukasi kesadaran Keamanan Informasi (*security awareness*);
2. pelaksanaan pengujian kerentanan dan keamanan sistem (*Vulnerability Assessment and Penetration Testing*/VAPT);
3. peningkatan arsitektur Keamanan Informasi;
4. penanganan Insiden Siber; dan
5. Audit Keamanan Informasi.

Program kerja Keamanan Informasi dituangkan dalam Peta Rencana Keamanan Informasi yang disusun untuk periode 5 (lima) tahunan dengan menetapkan sasaran Keamanan Informasi setiap tahunnya. Peta Rencana Keamanan Informasi sebagaimana dimaksud menjadi bagian yang tidak terpisahkan dari Peta Rencana SPBE KP2MI/BP2MI.

BAB IV
DUKUNGAN PENGOPERASIAN

A. Sekretaris Jenderal memberikan dukungan terhadap penyelenggaraan Keamanan Informasi dengan mengalokasikan sumber daya manusia Keamanan Informasi yang berkompeten serta anggaran Keamanan Informasi yang memadai.

B. Sumber daya manusia Keamanan Informasi yang dialokasikan sebagaimana dimaksud pada huruf A wajib memiliki standar kompetensi paling sedikit di bidang:
   1. Keamanan Infrastruktur Teknologi Informasi dan Komunikasi (TIK); dan
   2. Keamanan Aplikasi.

C. Dalam hal sumber daya manusia keamanan informasi yang dialokasikan belum memiliki kompetensi yang memadai, maka Sekretaris Jenderal memfasilitasi program peningkatan kompetensi melalui kegiatan pelatihan, sertifikasi, dan/atau bimbingan teknis.

D. Sekretaris Jenderal bersama Tim SMKI memfasilitasi penyelenggaraan kegiatan peningkatan kesadaran Keamanan Informasi (*security awareness*) bagi seluruh pegawai di lingkungan KP2MI/BP2MI secara berkala.

E. Sekretaris Jenderal menyediakan anggaran Keamanan Informasi berdasarkan arsitektur dan peta rencana Keamanan Informasi yang telah disusun.

F. Anggaran Keamanan Informasi dibebankan pada Daftar Isian Pelaksanaan Anggaran (DIPA) KP2MI/BP2MI atau sumber lainnya yang sah dan tidak mengikat sesuai ketentuan peraturan perundang-undangan.

BAB V
KEAMANAN SUMBER DAYA MANUSIA

Keamanan sumber daya manusia diselenggarakan untuk memastikan bahwa seluruh pegawai dan pihak ketiga memahami, mematuhi, serta memegang tanggung jawab penuh terhadap pelindungan aset informasi di lingkungan KP2MI/BP2MI. Pengelolaan keamanan sumber daya manusia dilaksanakan oleh Tim SMKI berkoordinasi dengan unit kerja yang membidangi urusan sumber daya manusia dan unit kerja terkait lainnya, dengan ruang lingkup yang meliputi:

A. mengomunikasikan peran dan tanggung jawab pelaksanaan Kebijakan SMKI kepada seluruh pegawai dan pihak ketiga yang terlibat dalam pengelolaan serta pengamanan aset informasi;
B. menerapkan prinsip pemisahan tugas dan wewenang (*segregation of duties*) untuk memitigasi risiko kesalahan, penyalahgunaan, atau pelanggaran keamanan;
C. melakukan pemeriksaan latar belakang (*background screening*) secara proporsional terhadap pegawai dan pihak ketiga yang akan diberikan hak akses ke dalam Sistem Elektronik yang bersifat sensitif atau kritikal;
D. mewajibkan penandatanganan Perjanjian Kerahasiaan (*Non-Disclosure Agreement*/NDA) bagi pegawai dan pihak ketiga yang terlibat dalam penggunaan dan/atau pengelolaan informasi, yang memuat tanggung jawab pelindungan data serta sanksi atas pelanggaran Keamanan Informasi;
E. menangguhkan hak penggunaan aset informasi bagi pegawai yang sedang dalam masa pemeriksaan akibat dugaan pelanggaran Keamanan Informasi;
F. mencabut seluruh hak akses terhadap aset informasi apabila pegawai atau pihak ketiga tidak lagi memiliki kepentingan operasional, dimutasi, atau telah mengakhiri masa tugasnya di KP2MI/BP2MI;
G. menyusun Berita Acara Serah Terima (BAST) untuk memastikan pengembalian seluruh aset informasi yang dipergunakan selama bekerja dari pegawai yang purnatugas, berhenti bekerja, atau dimutasi;
H. menyelenggarakan program edukasi kesadaran Keamanan Informasi (*security awareness*) melalui kegiatan sosialisasi, bimbingan teknis, dan/atau pelatihan yang dilaksanakan secara berkala; dan
I. mendokumentasikan serta memelihara rekam jejak pelatihan, kompetensi, pengalaman, dan kualifikasi bagi pegawai yang ditugaskan mengelola Keamanan Informasi.

BAB VI
KEAMANAN ASET

Pengelolaan keamanan aset diselenggarakan untuk melindungi seluruh Perangkat Keras, Perangkat Lunak, serta Data dan Informasi berdasarkan klasifikasi dan tingkat kritikalitasnya. Pelaksanaan keamanan aset di lingkungan KP2MI/BP2MI dikelola oleh Tim SMKI berkoordinasi dengan unit kerja terkait, dengan ruang lingkup yang meliputi:

A. mengidentifikasi dan mendokumentasikan aset Informasi ke dalam daftar inventaris aset yang memuat klasifikasi, tingkat kritikalitas, dan pihak yang bertanggung jawab (*asset owner*) atas setiap aset tersebut;
B. menerapkan pelabelan (*labeling*) pada aset Informasi sesuai dengan tingkat klasifikasi dan kritikalitasnya;
C. menetapkan hak akses terhadap aset Informasi berdasarkan kewenangan dan prinsip kebutuhan pekerjaan (*need-to-know basis*);
D. menetapkan pedoman aturan penggunaan aset Informasi (*acceptable use policy*) yang aman dan mengikat bagi seluruh pengguna;
E. menempatkan dan melindungi aset Informasi fisik di lokasi yang aman guna memitigasi risiko akses, pencurian, atau gangguan dari pihak yang tidak berwenang;
F. memastikan bahwa perpindahan atau penggunaan aset Informasi di luar lingkungan pusat data atau area layanan resmi telah mendapatkan persetujuan dari pimpinan unit kerja yang membidangi pengamanan data dan informasi;
G. melakukan proses sanitasi data (*data wiping/clearing*) terhadap perangkat penyimpanan media elektronik yang sudah tidak digunakan, sebelum perangkat tersebut dialihfungsikan atau dimusnahkan;
H. melaksanakan pemusnahan perangkat penyimpanan data fisik secara aman sesuai dengan standar dan prosedur operasional pemusnahan perangkat yang berlaku;
I. menghapus Informasi secara aman apabila tidak lagi diperlukan, masa retensinya berakhir, terdapat permintaan penghapusan yang sah, atau media akan dialihkan, dengan metode yang dapat diverifikasi dan dokumentasi pelaksanaannya;
J. mengelola secara khusus setiap aset Informasi yang memuat data pribadi atau informasi sensitif sesuai dengan ketentuan peraturan perundang-undangan di bidang pelindungan data pribadi; dan
K. melaksanakan manajemen aset Teknologi Informasi dan Komunikasi (TIK) sesuai dengan pedoman yang ditetapkan oleh kementerian yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

BAB VII
KEAMANAN AKSES

Pengelolaan pengendalian akses diselenggarakan untuk memastikan bahwa hak akses ke Sistem Elektronik, jaringan, dan informasi hanya diberikan kepada pengguna yang sah serta berwenang guna memitigasi risiko akses tanpa hak. Pelaksanaan pengendalian akses di lingkungan KP2MI/BP2MI dikelola oleh Tim SMKI berkoordinasi dengan Pemilik Proses Bisnis dan unit kerja terkait, dengan ruang lingkup yang meliputi:

A. menyusun prosedur pengelolaan hak akses pengguna berdasarkan kebutuhan organisasi, persyaratan keamanan, dan ketentuan peraturan perundang-undangan;
B. pengelolaan hak akses pengguna:
   1. menetapkan kewajiban setiap pengguna untuk menjaga kerahasiaan kredensial, akun, kata sandi (*password*), PIN, OTP, dan token autentikasi masing-masing, serta bertanggung jawab penuh atas segala aktivitas yang terjadi menggunakan akun miliknya;
   2. mewajibkan pengguna untuk segera melaporkan dugaan penyalahgunaan atau kompromi akun kepada pengelola teknis, serta segera melakukan penggantian informasi autentikasi;
   3. memastikan alokasi dan penggunaan identitas akun yang unik (*unique user ID*) untuk setiap pengguna yang hanya digunakan untuk melaksanakan tugas sesuai dengan kewenangan yang diberikan;
   4. mencegakkan larangan berbagi kredensial, di mana pengguna dilarang keras menggunakan akun milik orang lain, mengizinkan pihak lain menggunakan akun miliknya, serta dilarang memberikan, memperlihatkan, atau mengirimkan informasi autentikasi kepada siapa pun, termasuk kepada atasan, rekan kerja, administrator sistem, maupun pihak ketiga;
   5. membatasi dan mengendalikan pemberian hak akses khusus (*privileged access*) secara ketat hanya untuk pengguna yang memiliki kewenangan operasional tertentu;
   6. mengelola dan menerapkan standar konfigurasi kata sandi pengguna sesuai dengan ketentuan yang ditetapkan;
   7. memantau, mengevaluasi, dan meninjau ulang (*review*) hak akses pengguna secara berkala paling sedikit 1 (satu) kali dalam 6 (enam) bulan;
   8. memelihara catatan log aktivitas pengguna (*user log*) sebagai pemenuhan aspek akuntabilitas; dan
   9. menonaktifkan atau mencabut hak akses pengguna secara seketika bagi pegawai atau pihak ketiga yang telah berakhir masa penugasannya, dimutasi, atau purna tugas;
C. pengendalian akses jaringan dan layanan jaringan:
   1. menerapkan mekanisme otorisasi yang ketat untuk setiap permintaan koneksi ke dalam jaringan internal organisasi;
   2. membatasi akses ke infrastruktur jaringan dan aplikasi diagnosis sistem hanya untuk pegawai teknis yang bertugas melakukan pengujian, pemecahan masalah, atau pengembangan sistem;
   3. memberikan akses jaringan kepada tamu (*guest network*) secara terbatas, terisolasi, dan dalam jangka waktu tertentu;
   4. menerapkan pembatasan masa aktif sesi (*session time-out*) dan/atau batas waktu koneksi (*connection time limit*) pada sistem elektronik maupun antarmuka koneksi jarak jauh guna mengelola kapasitas sumber daya dan mencegah akses yang ditinggalkan (*idle session*);

5. melakukan pemantauan lalu lintas jaringan (*network traffic monitoring*) secara terpusat terhadap pengguna aktif pada jaringan internal guna mendeteksi anomali, penyalahgunaan, dan potensi ancaman siber secara dini; dan
6. melakukan pemutusan atau penghentian layanan jaringan pada segmen atau area yang terindikasi mengalami gangguan keamanan informasi atau serangan siber;

D. pengendalian akses Aplikasi dan Sistem Informasi:
1. memastikan otorisasi identitas pengguna wajib menggunakan teknik autentikasi yang aman dan terstandar guna memvalidasi identitas digital pengguna;
2. mengaktifkan fasilitas batas waktu sesi (*session time-out*) yang secara otomatis menutup atau mengunci layar komputer, aplikasi, serta koneksi jaringan apabila tidak terdapat aktivitas pengguna dalam periode waktu yang ditentukan;
3. menerapkan pembatasan waktu koneksi (*connection time limit*) khusus untuk sistem informasi dan aplikasi yang mengelola data berklasifikasi rahasia;
4. melindungi penyimpanan aset informasi yang memuat data pribadi menggunakan teknologi kriptografi (*enkripsi*) serta pembatasan akses yang ketat; dan
5. membatasi akses ke kode sumber (*source code*) aplikasi secara ketat dan hanya diperuntukkan bagi pengembang sistem yang sah melalui jalur repositori yang aman;

E. pengendalian perangkat kerja jarak jauh (*remote working*) dengan cara menentukan parameter keamanan yang wajib dipenuhi setiap perangkat yang digunakan untuk mengakses aset Informasi dari luar lingkungan KP2MI/BP2MI, yang terdiri dari namun tidak terbatas pada:
1. *Virtual Private Network* (VPN);
2. *Transport Layer Security/ Secure Socket Layer* (TLS/SSL); dan/atau
3. *Multi-Factor Authentication* (MFA)/ *Two-Factor Authentication* (2FA);

F. pengelolaan Hak Akses Khusus (*Privileged Access Rights*):
1. mengidentifikasi hak akses khusus untuk dialokasikan kepada pengguna terkait;
2. memberikan hak akses khusus hanya kepada pengguna sesuai dengan peruntukannya berdasarkan kebutuhan dan kegiatan tertentu;
3. mengelola proses otorisasi dan mendokumentasikan catatan penggunaan atas seluruh hak akses khusus; dan
4. memberikan hak akses khusus secara terpisah dari akun yang digunakan untuk kegiatan umum;

G. pemantauan akses Sistem Elektronik meliputi:
1. kegagalan akses;
2. penggunaan hak akses tidak wajar;
3. alokasi dan penggunaan hak akses khusus;
4. penelusuran transaksi pengiriman *file* sistem atau dokumen tertentu yang mencurigakan; dan
5. penggunaan sumber daya sensitif; dan

H. menghapus akun setiap pegawai dan pihak ketiga yang tidak lagi memiliki kepentingan terhadap akses aset Informasi, dimutasi, berhenti, atau telah berakhir kontraknya.

BAB VIII
KEAMANAN KRIPTOGRAFI

Pengelolaan keamanan kriptografi diselenggarakan untuk memastikan penggunaan teknik kriptografi yang tepat guna melindungi kerahasiaan, keutuhan, dan keautentikan data serta informasi yang dikelola. Pelaksanaan keamanan kriptografi di lingkungan KP2MI/BP2MI dikelola oleh Tim SMKI berkoordinasi dengan unit kerja terkait, dengan ruang lingkup yang meliputi:

A. melakukan klasifikasi informasi yang disimpan dan dikelola dalam perangkat teknologi informasi sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.
B. menerapkan mekanisme keamanan kriptografi untuk informasi berklasifikasi rahasia dan/atau sangat rahasia dengan cara :
    1. menerapkan jalur komunikasi aman dengan menerapkan *Transport Layer Security/Secure Socket Layer (*TLS/SSL*)* untuk proses autentikasi antara pengguna dengan Aplikasi berbasis website;
    2. menjaga kerahasiaan kata sandi dan menyimpannya dalam basis data dengan mekanisme *hash function*;
    3. melindungi kerahasiaan data dan Informasi rahasia dan/atau sangat rahasia yang dipertukarkirimkan dan disimpan dalam basis data dengan melakukan enkripsi;
    4. menerapkan autentikasi berbasis Tanda Tangan Elektronik (TTE) dengan menggunakan sertifikat elektronik yang dikeluarkan oleh Penyelenggara Sertifikat Elektronik (PSrE) yang sah dan terakreditasi; dan
    5. menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan peraturan perundangan dan/atau rekomendasi dari Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber; dan
C. mengintegrasikan perangkat lunak atau modul kriptografi yang telah tersertifikasi oleh Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber ke dalam sistem aplikasi strategis KP2MI/BP2MI guna menjamin kekuatan enkripsi yang sesuai dengan standar negara.

BAB IX
KEAMANAN FISIK DAN LINGKUNGAN

Pengelolaan keamanan fisik dan lingkungan diselenggarakan untuk memberikan pelindungan, pemeliharaan, serta menjamin ketersediaan aset infrastruktur teknologi informasi dan komunikasi dari ancaman fisik, lingkungan, dan bencana. Pelaksanaan keamanan fisik dan lingkungan di lingkungan KP2MI/BP2MI dikelola oleh Tim SMKI berkoordinasi dengan unit kerja terkait, meliputi:

A. menyimpan Infrastruktur di ruangan khusus yang dilindungi dengan pengamanan fisik yang memadai meliputi :
   1. pintu dengan kontrol akses;
   2. kamera pengawas (CCTV);
   3. pendeteksi asap;
   4. sistem pemadam kebakaran; dan
   5. perangkat pemutus aliran listrik;
B. membatasi akses masuk ke pusat data dan area kerja layanan informasi yang berisi data dan/atau Informasi rahasia dan/atau sangat rahasia hanya bagi pegawai yang memiliki wewenang;
C. melaksanakan pemantauan keamanan fisik terhadap area terbatas dan fasilitas pemrosesan Informasi melalui kamera pengawas, alarm, log akses, dan/atau mekanisme lain yang sesuai serta rekaman diproteksi, direviu, dan disimpan berdasarkan kebutuhan keamanan, privasi, dan retensi;
D. mewajibkan pendampingan oleh pegawai yang ditugaskan waktu kunjungan pihak ketiga yang memasuki pusat data dan/atau area kerja layanan Informasi yang berisikan data dan/atau informasi rahasia dan/atau sangat rahasia;
E. menerapkan larangan membawa masuk dan mengkonsumsi makanan dan minuman di dalam ruang *server* Pusat Data;
F. menetapkan semua area yang digunakan untuk menyimpan aset Informasi merupakan area bebas rokok;
G. pengamanan area pusat data dan area kerja layanan informasi dilakukan sesuai prosedur keamanan area;
H. melaksanakan pengamanan kantor, ruangan, dan fasilitas kerja sesuai dengan peraturan dan standar keamanan dan keselamatan kerja, termasuk *clear screen policy* dan *clean desk policy*;
I. memastikan perangkat pemadam kebakaran wajib disediakan, dipelihara, dan diletakkan di tempat yang mudah dijangkau di area pusat data maupun lingkungan kerja;
J. memelihara infrastruktur yang digunakan untuk menjalankan aplikasi sesuai dengan buku petunjuk teknis atau panduan resmi pabrikan;
K. memantau dan mengawasi kondisi suhu serta kelembapan di dalam ruang server pusat data secara berkala sesuai batas minimum dan maksimum yang disyaratkan oleh pabrikan perangkat;
L. memastikan seluruh infrastruktur mendapatkan pasokan daya listrik yang stabil dan sesuai dengan spesifikasi teknis perangkat;
M. menyediakan sumber daya listrik alternatif (*back-up power*) berupa generator listrik dan *Uninterruptible Power Supply* (UPS) dengan konfigurasi yang mampu mengalihkan pasokan daya tanpa menimbulkan gangguan atau interupsi pada infrastruktur;
N. mengamankan jalur kabel di pusat data dan area kerja layanan informasi dengan mengikuti standar mekanikal dan elektrikal pusat data yang berlaku;

O. memosisikan infrastruktur yang menangani informasi sensitif sedemikian rupa guna meminimalisasi sudut pandang dari pihak yang tidak berwenang (*shoulder surfing*);
P. menerapkan sistem proteksi petir pada bangunan pusat data serta memasang filter perlindungan petir pada jalur komunikasi dan kelistrikan;
Q. memastikan bahwa dalam hal pemeliharaan infrastruktur TIK tidak dapat dilakukan di tempat, maka pemindahan infrastruktur dilakukan berdasarkan persetujuan Kepala Unit Organisasi yang membidangi data dan informasi;
R. memastikan data dan informasi berklasifikasi rahasia dan/atau sangat rahasia yang tersimpan pada perangkat telah dipindahkan ke media penyimpanan lain, dan dilakukan penghapusan aman (*secure wiping*) pada media penyimpanan asal sebelum perangkat dipindahkan ke luar lingkungan kerja;
S. mewajibkan pembuatan perjanjian kerja sama yang memuat klausul kerahasiaan (*Non-Disclosure Agreement*), ruang lingkup pemeliharaan, serta komitmen tingkat layanan (*Service Level Agreement*) apabila pemeliharaan infrastruktur melibatkan pihak ketiga;
T. menempatkan infrastruktur, perangkat pemulihan, dan media penyimpanan data cadangan (*back-up media*) di lokasi aman dengan struktur bangunan yang memadai untuk menghindari kerusakan akibat hama, faktor lingkungan, dan bencana alam; dan
U. menyimpan bahan berbahaya atau mudah terbakar pada jarak yang aman dan terisolasi dari area pusat data serta area kerja layanan informasi.

BAB X
KEAMANAN OPERASIONAL

Pengelolaan keamanan operasional diselenggarakan untuk memastikan implementasi, pengoperasian, dan pemeliharaan fasilitas pengolah informasi berjalan secara aman, meminimalkan risiko kegagalan, serta melindungi keutuhan aset informasi. Pelaksanaan keamanan operasional di lingkungan KP2MI/BP2MI dikelola oleh Tim SMKI berkoordinasi dengan unit kerja terkait, dengan ruang lingkup yang meliputi:

A. mendokumentasikan, memelihara, dan menyediakan prosedur pengoperasian perangkat informasi sesuai dengan peruntukannya;
B. menyusun, mengevaluasi, dan memutakhirkan katalog serta standar teknologi keamanan informasi yang disetujui untuk diimplementasikan di lingkungan KP2MI/BP2MI;
C. menyusun kebijakan dan persyaratan keamanan informasi untuk penggunaan layanan komputasi awan (*cloud services*) serta mengevaluasi kepatuhan pihak penyedia layanan;
D. mengendalikan dan mendokumentasikan setiap perubahan pada aset informasi yang dapat memengaruhi keamanan informasi dengan memperhatikan manajemen risiko serta persetujuan dari pemilik aset (*asset owner*);
E. menetapkan kriteria penerimaan (*acceptance criteria*) untuk sistem informasi baru, pemutakhiran, maupun versi baru, serta melakukan pengujian komprehensif sebelum dioperasikan;
F. memantau penggunaan aset informasi serta membuat proyeksi kebutuhan kapasitas ke depan guna menjamin ketersediaan layanan, khususnya pada aset informasi yang bersifat kritikal;
G. melakukan pemisahan akses terhadap Informasi yang memiliki klasifikasi rahasia dan/atau sangat rahasia (seorang pegawai dihindari memiliki akses terhadap seluruh aset Informasi dan perangkat pengolahnya);
H. memisahkan secara ketat lingkungan pengembangan (*development*), lingkungan pengujian (*testing/staging*), dan lingkungan operasional (*production*) untuk mengurangi risiko perubahan tanpa izin pada sistem operasional;
I. menerapkan sistem pendeteksian, pencegahan, dan pemulihan sebagai bentuk perlindungan terhadap ancaman *malware*;
J. mengonfigurasi dan memperbarui perangkat keamanan paling sedikit meliputi:
    1. perangkat *firewall*;
    2. perangkat *Intrusion Prevention System* (IPS);
    3. perangkat antivirus;
    4. perangkat manajemen akses pengguna; dan
    5. perangkat monitoring/pendukung lainnya sesuai perkembangan teknologi Keamanan Informasi;
K. menetapkan, menerapkan, dan memantau secara ketat manajemen konfigurasi (*configuration management*) yang aman untuk seluruh perangkat keras, perangkat lunak, layanan, dan jaringan guna mencegah kerentanan akibat kesalahan konfigurasi;
L. menerapkan sistem dan teknologi pencegahan kebocoran data (*Data Leakage Prevention*/DLP) pada sistem, jaringan, dan perangkat titik akhir (*endpoint*) untuk mendeteksi dan mencegah ekstraksi atau transmisi informasi sensitif secara tidak sah;

M. melakukan penilaian kerentanan terhadap perangkat informasi (*vulnerability assessment*) secara berkala dan melakukan tindakan perlindungan terhadap kerentanan dan/atau ancaman yang teridentifikasi;

N. melakukan pembuatan, penyimpanan, dan pengujian salinan cadangan (*backup*) Informasi dan aplikasi yang berada di pusat data dan/atau area kerja layanan Informasi secara berkala sesuai dengan prosedur *backup* di KP2MI/BP2MI;

O. mencatat dan memelihara log setiap aktivitas administrator, aktivitas pengguna, peristiwa kegagalan, dan kejadian keamanan serta disimpan dalam periode tertentu;

P. menerapkan pencatatan kesalahan sistem (*error logging*) untuk dianalisis dan diambil tindakan pengamanan atau perbaikan yang tepat;

Q. melindungi seluruh sistem pencatatan log dari upaya pemalsuan, modifikasi, penghapusan, maupun akses yang tidak berwenang;

R. memastikan semua perangkat pengolah informasi yang tersambung dengan jaringan telah disinkronisasi dengan sumber waktu yang akurat (*Network Time Protocol*/NTP) yang disepakati;

S. menyusun, menerapkan, dan memutakhirkan Pernyataan Penerapan (*Statement of Applicability*/SoA) kontrol keamanan informasi beserta justifikasi pemilihan atau pengecualian kontrol;

T. menyusun pedoman manajemen kapasitas sistem elektronik dan mengevaluasi laporan utilisasi sumber daya Teknologi Informasi (komputasi, penyimpanan, dan jaringan) untuk memastikan ketersediaan layanan;

U. mendokumentasikan, memelihara, dan mengevaluasi kepatuhan penerapan standar konfigurasi aman (*secure baseline configuration*) pada perangkat dan sistem informasi sesuai dengan perkembangan ancaman; dan

V. menerapkan audit logging yang mencatat aktivitas pengguna dan kejadian Keamanan Informasi dalam kurun waktu tertentu untuk membantu investigasi di masa mendatang, terdiri atas:
   1. kegagalan akses;
   2. penggunaan hak akses tidak wajar;
   3. alokasi dan penggunaan hak akses khusus;
   4. penelusuran transaksi pengiriman file sistem atau dokumen tertentu yang mencurigakan; dan
   5. penggunaan sumber daya sensitif.

BAB XI
KEAMANAN KOMUNIKASI

Pengelolaan keamanan komunikasi diselenggarakan untuk menjamin pelindungan data dan informasi yang ditransmisikan melalui jaringan komunikasi internal maupun publik. Pelaksanaan keamanan komunikasi di lingkungan KP2MI/BP2MI dikelola oleh Tim SMKI berkoordinasi dengan unit kerja terkait, dengan ruang lingkup yang meliputi:

A. mengidentifikasi fitur keamanan layanan, tingkat layanan, dan kebutuhan pengelolaan dalam setiap kesepakatan penyediaan layanan jaringan, termasuk layanan yang disediakan oleh pihak ketiga;
B. menyusun standar arsitektur jaringan yang aman dan memastikan penerapannya (seperti segmentasi jaringan, pemfilteran akses, dan zona kepercayaan) oleh tim teknis operasional;
C. menerapkan kontrol penyaringan akses web (*web filtering*) untuk mencegah dan membatasi pengguna dalam mengakses situs web eksternal yang mengandung kode berbahaya, ilegal, atau tidak sesuai dengan aturan penggunaan aset (*acceptable use policy*) KP2MI/BP2MI;
D. melakukan pemantauan serta pencatatan aktivitas secara ketat dalam hal pihak ketiga diizinkan untuk mengakses jaringan internal;
E. melindungi jaringan dari pihak yang tidak berhak mengakses, paling sedikit meliputi:
    1. mendokumentasikan arsitektur jaringan secara komprehensif, yang meliputi seluruh komponen infrastruktur dan aplikasi jaringan;
    2. menerapkan teknologi keamanan jaringan berbasis enkripsi dan autentikasi, termasuk penggunaan Sertifikat Elektronik;
    3. menerapkan pemisahan (*segregation/segmentation*) jaringan untuk kelompok pengguna, layanan informasi, dan sistem informasi guna melindungi jaringan dari pihak yang tidak berhak;
    4. menerapkan parameter teknis yang diperlukan untuk memastikan koneksi yang aman dengan layanan jaringan; dan
    5. menerapkan prosedur penggunaan layanan jaringan yang membatasi akses tanpa hak ke layanan jaringan atau aplikasi;
F. menetapkan prosedur pertukaran informasi yang mengatur spesifikasi sistem dan standar keamanan yang digunakan untuk proses pertukaran informasi;
G. memastikan bahwa seluruh transmisi data yang bersifat rahasia dilakukan melalui kanal komunikasi aman yang telah mendapatkan validasi atau sertifikasi dari Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber;
H. menetapkan prosedur penanganan permintaan informasi dari pihak eksternal yang meliputi:
    1. mekanisme verifikasi identitas pemohon dan validitas kepentingan permintaan data;
    2. mekanisme klasifikasi data untuk memastikan bahwa data yang diminta merupakan data publik yang diperbolehkan untuk diakses, atau data dikecualikan (rahasia) sesuai dengan ketentuan peraturan perundang-undangan di bidang keterbukaan informasi publik dan pelindungan data pribadi;
    3. kewajiban mendapatkan persetujuan tertulis dari pemilik data (*data owner*) atau pimpinan unit kerja terkait sebelum data diserahkan kepada pihak eksternal; dan

4. pencatatan (*logging*) atas setiap penyerahan data kepada pihak eksternal sebagai bagian dari audit trail untuk pemenuhan akuntabilitas;

I. melindungi informasi di dalam aplikasi yang ditransmisikan melewati jaringan publik dari upaya pengungkapan, modifikasi, dan perusakan dengan menerapkan mekanisme kriptografi;

J. memberikan pelindungan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (*non-repudiation*) untuk informasi elektronik yang berklasifikasi rahasia dan/atau sangat rahasia; dan

K. melakukan pendeteksian dan perlindungan berlapis terhadap kode berbahaya (*malicious code*) yang mungkin disisipkan pada file yang dikirimkan melalui Sistem Elektronik.

BAB XII
KEAMANAN PENGEMBANGAN DAN PEMELIHARAAN

Pengelolaan keamanan pengembangan dan pemeliharaan sistem diselenggarakan untuk memastikan bahwa keamanan informasi menjadi bagian yang terintegrasi dalam daur hidup aset informasi (*System Development Life Cycle*/SDLC) guna mencegah terjadinya kesalahan, eksploitasi, modifikasi, dan perusakan oleh pihak yang tidak berwenang. Pelaksanaan keamanan pengembangan dan pemeliharaan di lingkungan KP2MI/BP2MI dikelola oleh Tim SMKI berkoordinasi dengan unit kerja terkait, dengan ruang lingkup yang meliputi:

A. memisahkan lingkungan pengembangan (*development*), lingkungan pengujian (*testing*), dan lingkungan operasional (*production*) aplikasi, baik secara fisik, logis, maupun hak aksesnya;
B. menjaga dan memastikan agar lingkungan pengembangan tidak dapat diakses dari sistem operasional layanan;
C. mengupayakan agar arsitektur dan konfigurasi lingkungan pengujian dibuat sama atau merepresentasikan lingkungan operasional layanan;
D. memilih data uji (*test data*) secara hati-hati, serta melindungi dan mengendalikannya guna mencegah kebocoran informasi sensitif;
E. memastikan bahwa proses perencanaan, pembangunan, dan pengembangan aplikasi maupun infrastruktur termasuk yang dilakukan oleh pihak ketiga telah memasukkan fitur-fitur keamanan ke dalam spesifikasi sistem (*security by design*);
F. menerapkan prinsip dan pedoman pengkodean yang aman (*secure coding*) dalam seluruh siklus pengembangan aplikasi untuk meminimalkan kerentanan perangkat lunak;
G. menerapkan teknik penyelubungan data (*data masking*), anonimisasi, tokenisasi, pseudonimisasi atau teknik lain yang sepadan untuk melindungi data pribadi dan informasi sensitif, khususnya ketika data tersebut digunakan pada lingkungan pengujian (*testing environment*);
H. menerapkan fitur-fitur keamanan yang minimal memenuhi standar keamanan yang ditetapkan oleh lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber, yang mencakup pemenuhan terhadap:
    1. standar keamanan data dan informasi;
    2. standar keamanan aplikasi;
    3. standar keamanan pusat data;
    4. standar keamanan sistem penghubung layanan; dan
    5. standar keamanan jaringan intra;
I. melaksanakan pembangunan dan pengembangan aplikasi sesuai dengan standar teknis dan prosedur yang ditetapkan oleh kementerian yang menyelenggarakan tugas pemerintahan di bidang komunikasi dan informatika;
J. mengawasi dan memantau seluruh aktivitas pembangunan dan pengembangan aplikasi dan infrastruktur yang dialihdayakan kepada pihak ketiga;
K. melaksanakan uji kelaikan Aplikasi secara komprehensif sebelum aplikasi digunakan dan sewaktu-waktu sesuai kebutuhan, yang mencakup aspek:
    1. uji fungsi (*functional testing*), dilakukan untuk memastikan aplikasi yang dibangun dan/atau dikembangkan telah memenuhi fungsi-fungsi sesuai dengan dokumentasi terkait;

2. uji integrasi (*integration testing*), dilakukan untuk yang memastikan aplikasi yang dibangun dan/atau dikembangkan telah memenuhi kebutuhan dan persyaratan integrasi dengan aplikasi, data, serta komponen-komponen lain yang terkait;
3. uji beban (*load/stress testing*), dilakukan untuk yang memastikan Aplikasi yang dibangun dan/atau dikembangkan dapat berfungsi sebagaimana mestinya menghadapi beban kerja yang dikenakan terhadapnya; dan
4. uji keamanan*(security testing)*, dilakukan untuk memastikan Aplikasi yang dibangun dan/atau dikembangkan dapat menjaga keamanan data dan Informasi yang terkait dengannya;

L. menggunakan pedoman atau instrumen pengukuran yang ditetapkan oleh kementerian yang menyelenggarakan urusan di bidang komunikasi dan informatika dalam pelaksanaan uji fungsi, uji integrasi, dan uji beban; dan

M. menggunakan pedoman atau instrumen pengukuran yang ditetapkan oleh lembaga yang menyelenggarakan urusan di bidang keamanan siber dalam pelaksanaan uji keamanan aplikasi.

BAB XIII
KEAMANAN PIHAK KETIGA

Pengelolaan keamanan pihak ketiga diselenggarakan untuk memastikan pelindungan berlapis terhadap aset informasi yang diakses, dikelola, atau digunakan oleh pihak ketiga dalam pelaksanaan kerja sama. Pelaksanaan keamanan pihak ketiga di lingkungan KP2MI/BP2MI dikelola oleh Tim SMKI berkoordinasi dengan unit kerja terkait, meliputi:

A. melakukan pemeriksaan latar belakang (*background screening*) terhadap pihak ketiga dengan tetap memperhatikan ketentuan peraturan perundang-undangan di bidang pelindungan data pribadi;
B. menyusun dan meninjau ulang secara berkala perjanjian keamanan tertulis dengan pihak ketiga yang terlibat dalam pengelolaan aset informasi, yang sekurang-kurangnya memuat klausul mengenai:
   1. perlindungan atas Informasi rahasia dan/atau sangat rahasia dan Hak Kekayaan Intelektual (HKI) setiap pihak;
   2. jaminan bebas dari kode berbahaya (*malicious code*) dan pintu belakang (*backdoor*) pada aset informasi yang disediakan oleh pihak ketiga;
   3. hak organisasi untuk melakukan audit dan pemantauan aktivitas yang melibatkan informasi rahasia dan/atau sangat rahasia;
   4. pengawasan dan pembatasan atas hak akses terhadap aset Informasi yang diberikan pada pihak ketiga;
   5. kewajiban pelaporan terhadap penyingkapan yang dilakukan secara tidak sah atau pelanggaran terhadap kerahasiaan;
   6. ketentuan pengembalian atau pemusnahan aset informasi secara aman pada saat masa berlaku perjanjian berakhir;
   7. penggunaan jalur komunikasi yang aman untuk perpindahan informasi antara KP2MI/BP2MI dengan pihak ketiga; dan
   8. penyerahan aset informasi yang dikuasainya oleh pihak ketiga kepada Tim SMKI pada saat pihak ketiga tidak lagi menjadi bagian dalam pengelolaan aset Informasi;
C. menetapkan persyaratan keamanan informasi yang spesifik terkait perolehan, penggunaan, pengelolaan, dan penghentian layanan komputasi awan (*cloud services*) yang disediakan oleh pihak ketiga;
D. menetapkan dan menerapkan persyaratan keamanan informasi yang spesifik pada rantai pasok Teknologi Informasi dan Komunikasi (*ICT supply chain*) dari seluruh produk dan layanan yang digunakan oleh KP2MI/BP2MI;
E. mewajibkan pihak ketiga untuk memastikan bahwa sub-kontraktor, komponen perangkat lunak (termasuk *open-source*), dan infrastruktur bawaan yang mereka gunakan telah memenuhi standar keamanan yang setara dan terbebas dari kerentanan atau fungsi tersembunyi (*backdoor*);
F. mensyaratkan hak audit, pelaporan kerentanan berkelanjutan, dan visibilitas arsitektur dari pihak pengembang atau pemasok layanan TIK guna memitigasi risiko keamanan yang berasal dari pihak ketiga ke rantai pasok utama;
G. memastikan *Service Level Agreement* (SLA) pihak ketiga telah mengatur ketersediaan layanan dan penyelesaian insiden keamanan;
H. melakukan pemantauan dan evaluasi secara berkala terhadap kinerja penyediaan layanan, laporan, dan catatan aktivitas (*log*) yang disediakan oleh pihak ketiga secara berkala;

I. memastikan secara berkala bahwa pengendalian Keamanan Informasi, definisi layanan, dan tingkat layanan yang termuat dalam kesepakatan penyediaan layanan, telah diterapkan, dioperasikan, dan dipelihara oleh pihak ketiga;
J. mencatat dan mendokumentasikan setiap peristiwa keamanan, masalah operasional, kegagalan, dan gangguan yang terkait dengan layanan yang diberikan oleh pihak ketiga;
K. mengkaji bersama pihak ketiga setiap adanya indikasi gangguan keamanan informasi dan merumuskan langkah perbaikan;
L. melakukan penilaian ulang risiko layanan (*risk reassessment*) secara berkala dengan memperhatikan tingkat kritikalitas, proses bisnis yang terkait, dan dampak operasional apabila terjadi rencana perubahan layanan oleh pihak ketiga;
M. memastikan seluruh personel pihak ketiga dan tamu yang memasuki lingkungan pusat data maupun area kerja layanan informasi mematuhi standar keamanan fisik dan lingkungan yang berlaku;
N. mencabut seluruh hak akses terhadap aset informasi yang dimiliki oleh pihak ketiga apabila kerja sama telah berakhir atau personel yang bersangkutan tidak lagi ditugaskan di KP2MI/BP2MI; dan
O. menyusun Berita Acara Serah Terima (BAST) aset untuk memastikan pengembalian seluruh aset informasi yang dipergunakan oleh pihak ketiga setelah masa kontrak berakhir.

BAB XIV
MANAJEMEN INSIDEN SIBER

Pengelolaan manajemen insiden siber diselenggarakan untuk memastikan kesiapan organisasi dalam mendeteksi, menanggulangi, memulihkan, serta mengevaluasi dampak dari insiden siber secara cepat, tepat, dan terkoordinasi. Pelaksanaan manajemen insiden siber di lingkungan KP2MI/BP2MI dikelola oleh Tim SMKI berkoordinasi dengan unit kerja terkait, meliputi:

A. membentuk Tim Tanggap Insiden Siber (*Computer Security Incident Response Team*/CSIRT) organisasi yang bertugas melaksanakan pencegahan, penanggulangan, dan pemulihan Insiden Siber. Tim CSIRT memiliki fungsi meliputi :
   1. memberikan peringatan terkait Keamanan Siber;
   2. merumuskan panduan teknis;
   3. mencatat setiap laporan/aduan yang dilaporkan;
   4. melakukan pemilahan (*triage*) prioritas Insiden Siber sesuai dengan kriteria;
   5. melakukan koordinasi penanganan Insiden Siber dengan pihak yang berkepentingan; dan
   6. menyelenggarakan fungsi tambahan berupa penanganan kerentanan Sistem Elektronik, analisis artefak digital, pengamatan potensi ancaman, pendeteksian serangan, dan konsultasi kesiapan penanganan Insiden Siber;
B. melakukan registrasi Tim Tanggap Insiden Siber (*Computer Security Incident Response Team*/CSIRT) kepada Tim Tanggap Insiden Siber nasional serta memelihara validitas registrasinya;
C. melakukan pemeliharaan validitas dan registrasi ulang sebelum masa berlaku surat tanda register berakhir, yakni setiap 3 (tiga) tahun sekali, atau apabila terdapat perubahan struktur organisasi;
D. melaksanakan tindakan perencanaan, pencegahan, dan kesiapan terhadap Insiden Siber yang dilaksanakan oleh Tim Tanggap Insiden Siber meliputi:
   1. menyusun dan menetapkan Rencana Tanggap Insiden Siber (*Incident Response Plan*) dan Rencana Keberlangsungan Kegiatan (*Business Continuity Plan*) yang sudah disetujui oleh Pemilik Proses Bisnis;
   2. mengumpulkan, menganalisis, dan memanfaatkan intelijen ancaman (*threat intelligence*) dari berbagai sumber terpercaya untuk memberikan wawasan terkait ancaman siber yang relevan guna memitigasi risiko secara proaktif;
   3. melakukan penilaian kerentanan (*vulnerability assessment*) dan/atau uji penetrasi (*penetration testing*) secara berkala untuk menemukan celah keamanan pada aset Informasi;
   4. mengimplementasikan dan mengelola alat monitoring keamanan berupa *Security information and event management* (SIEM);
   5. melaksanakan pemantauan (*monitoring*) serta pendeteksian dini terhadap aktivitas serangan siber pada aset informasi;
   6. menyusun berbagai skenario penanganan insiden siber berdasarkan potensi ancaman dan tingkat dampak operasional; dan
   7. melakukan simulasi penanganan insiden siber (*cyber drill test*) secara berkala berdasarkan skenario yang telah disusun paling sedikit 1 (satu) kali dalam 2 (dua) tahun serta setelah perubahan signifikan pada layanan, teknologi, organisasi, atau profil risiko;

E. menyediakan jalur jalur pelaporan dan analisis Insiden Siber yang disediakan oleh Tim Tanggap Insiden Siber meliputi:
   1. memastikan tersedianya kontak pelaporan Insiden Siber yang dapat diakses oleh seluruh pegawai di KP2MI/BP2MI termasuk oleh pihak ketiga, serta memelihara daftar kontak internal, eksternal, sektoral, dan nasional dan melakukan uji komunikasi secara berkala;
   2. menerima, mencatat, dan mendokumentasikan setiap peringatan dini dari sistem pemantauan (*monitoring*) maupun laporan insiden siber yang masuk ke dalam sistem;
   3. melakukan triase (*triage*) dan analisis dampak Insiden Siber, baik yang bersumber dari pelaporan maupun hasil pemantauan, guna memprioritaskan penanganan berdasarkan tingkat kedaruratan, kategori Sistem Elektronik yang terdampak, dan kriteria risiko organisasi; dan
   4. menetapkan mekanisme pemberian peringatan dan pemberitahuan potensi ancaman kepada Pemilik Proses Bisnis dan pihak terkait;

F. melaksanakan prosedur penanganan Insiden Siber yang dilaksanakan oleh Tim Tanggap Insiden Siber meliputi:
   1. melaksanakan prosedur penanganan Insiden Siber meliputi fase persiapan, identifikasi, penahanan (*containment*), penghapusan/eradikasi penyebab insiden, pemulihan (*recovery*), dan tindak lanjut;
   2. memastikan Insiden Siber diisolasi dan dimitigasi secara cepat guna meminimalkan jangkauan kerusakan dan mencegah meluasnya eskalasi dampak;
   3. mengumpulkan, mengamankan, dan memelihara bukti elektronik atau artefak digital melalui prosedur forensik digital secara akuntabel guna keperluan investigasi dan penegakan hukum;
   4. melaksanakan prosedur pencadangan dan pemulihan sistem/data sesuai rencana keberlangsungan kegiatan, serta melakukan pengujian ulang terhadap fungsi vital untuk memastikan capaian target waktu pemulihan terpenuhi; dan
   5. memastikan organisasi memiliki dan mengelola strategi komunikasi publik untuk mengelola informasi yang disebarkan kepada media, pemangku kepentingan, maupun masyarakat saat dan setelah terjadinya Insiden Siber;

G. melaksanakan prosedur peningkatan keamanan pasca-insiden (*lesson learned*) yang dilaksanakan oleh Tim Tanggap Insiden Siber meliputi:
   1. menyusun laporan resmi penanganan insiden siber secara komprehensif setelah proses penanggulangan selesai dilakukan;
   2. mengevaluasi laporan hasil penanganan insiden serta melaksanakan analisis akar masalah (*root cause analysis*) melalui tinjauan pasca-insiden (*post-incident review*) guna mendokumentasikan pembelajaran (*lessons learned*); dan
   3. meninjau kembali dan memperbarui efektivitas kendali keamanan, standar, prosedur operasional (SOP), serta rencana tanggap insiden guna mencegah berulangnya kejadian serupa di masa mendatang;

H. menyampaikan dan mendiseminasikan informasi terkait Insiden Siber sebagai berikut:
   1. menyampaikan dan mendiseminasikan informasi Insiden Siber kepada pihak terdampak dengan menggunakan kode distribusi informasi *Traffic Light Protocol* (TLP) guna memfasilitasi pembagian informasi sensitif;

2. penggunaan label TLP meliputi pembatasan pengungkapan sebagai berikut:
   a) TLP:RED untuk mata dan telinga penerima individu saja, tidak ada pengungkapan lebih lanjut;
   b) TLP:AMBER untuk penyebaran terbatas berdasarkan kebutuhan untuk mengetahui (*need-to-know basis*) dalam organisasi dan pihak ketiga, atau
   c) TLP:AMBER+STRICT yang membatasi berbagi hanya untuk internal organisasi;
   d) TLP:GREEN untuk penyebaran terbatas di dalam komunitas keamanan siber terkait, tidak untuk publik; dan
   e) TLP:CLEAR untuk penyebaran tanpa batasan rilis publik;
3. pencantuman label TLP diwajibkan pada subjek pesan elektronik (*email*) dan diletakkan pada *header* serta *footer* setiap halaman untuk dokumen berformat fisik/digital; dan
4. informasi Insiden Siber hanya dibagikan kepada penerima dan dalam lingkup yang diperbolehkan oleh label TLP, klasifikasi informasi, dan ketentuan internal;

I. melaksanakan peningkatan kapasitas Sumber Daya Manusia Tim Tanggap Insiden Siber meliputi:
   1. memberikan pelatihan teknis penanganan Insiden Siber secara berkala bagi personel yang ditugaskan dalam keanggotaan CSIRT organisasi; dan
   2. menyelenggarakan program kesadaran keamanan siber (*security awareness*) bagi seluruh pegawai terkait cara mengenali ancaman dan prosedur pelaporan insiden; dan

J. melaksanakan pengukuran tingkat kematangan penerapan manajemen insiden siber (*maturity assessment*) secara periodik sesuai dengan instrumen dan pedoman yang ditetapkan oleh lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

BAB XV
MANAJEMEN KEBERLANGSUNGAN LAYANAN INFORMASI

Pengelolaan manajemen keberlangsungan layanan informasi diselenggarakan untuk menjamin ketersediaan, ketahanan, dan pemulihan layanan informasi seketika pada saat terjadi gangguan atau keadaan darurat. Pelaksanaan manajemen keberlangsungan layanan informasi di lingkungan KP2MI/BP2MI dikelola oleh Tim SMKI berkoordinasi dengan unit kerja terkait, meliputi:

A. melakukan identifikasi risiko dan analisis dampak bisnis (*business impact analysis*) terhadap keberlangsungan jalannya layanan informasi;
B. menyusun dan menerapkan rencana keberlangsungan layanan informasi (*Business Continuity Plan*/BCP) serta rencana pemulihan bencana (*Disaster Recovery Plan*/DRP) termasuk penetapan batas waktu pemulihan (*Recovery Time Objective*/RTO) dan titik pemulihan data (*Recovery Point Objective*/RPO) guna menjaga dan memulihkan operasional aset informasi dalam jangka waktu dan tingkat ketersediaan yang disepakati;
C. memastikan rencana keberlangsungan layanan informasi sekurang-kurangnya meliputi:
    1. memuat prosedur keberlangsungan layanan Informasi pada saat keadaan darurat, Manajemen Risiko, analisis dampak kegiatan, pengembalian kondisi sebelum terjadi gangguan peralihan kondisi normal, dan uji coba keberlangsungan kegiatan;
    2. menetapkan peran dan penanggung jawab pegawai yang terlibat dalam pelaksanaan keberlangsungan layanan Informasi; dan
    3. menyelenggarakan kegiatan sosialisasi dan pelatihan keberlangsungan layanan Informasi;
D. menerapkan mekanisme redundansi (*redundancy/high availability*) yang memadai pada infrastruktur aplikasi umum atau Sistem Elektronik yang berkategori strategis guna memastikan terpenuhinya target ketersediaan layanan informasi organisasi;
E. melaksanakan uji coba (*testing and exercising*) terhadap rencana keberlangsungan layanan informasi secara periodik untuk memastikan kesiapan dan efektivitas sistem pemulihan saat terjadi kedaruratan;
F. melaksanakan proses pemulihan dan pengaktifan jalur cadangan pada saat terjadi keadaan darurat sesuai dengan prosedur keberlangsungan layanan informasi yang telah ditetapkan;
G. menyusun prosedur keberlangsungan layanan informasi pada saat keadaan darurat, yang mencakup manajemen risiko, analisis dampak kegiatan, prosedur komunikasi krisis dan jalur notifikasi, pengembalian kondisi normal, dan uji coba keberlangsungan kegiatan; dan
H. memastikan seluruh pelaksanaan pengelolaan keberlangsungan layanan dilakukan selaras dengan pedoman manajemen layanan SPBE yang ditetapkan oleh kementerian yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

BAB XVI
PENGENDALIAN KEPATUHAN

Pengelolaan pengendalian kepatuhan diselenggarakan untuk memastikan bahwa seluruh penyelenggaraan keamanan informasi di lingkungan KP2MI/BP2MI memenuhi ketentuan peraturan perundang-undangan, komitmen kontraktual dengan pihak ketiga, serta selaras dengan kebijakan keamanan informasi yang ditetapkan. Pelaksanaan pengendalian kepatuhan di lingkungan KP2MI/BP2MI dikelola oleh Tim SMKI berkoordinasi dengan unit kerja terkait, meliputi:

A. mengidentifikasi, mendokumentasikan, mereviu, dan memelihara regulasi, standar, dan prosedur Keamanan Informasi;
B. memeriksa kepatuhan seluruh pegawai dan pihak ketiga secara berkala terhadap regulasi, standar, dan prosedur Keamanan Informasi;
C. memastikan pelindungan dan pengamanan privasi serta data pribadi yang dapat diidentifikasi sesuai dengan ketentuan peraturan perundang-undangan di bidang pelindungan data pribadi;
D. memastikan kesesuaian dan kepatuhan penerapan teknologi kriptografi dengan peraturan perundang-undangan yang berlaku;
E. memastikan seluruh rekaman dan dokumen penting organisasi terlindungi dari risiko kehilangan, kerusakan, pemalsuan, serta akses atau pengungkapan yang tidak sah sesuai persyaratan regulasi dan kebutuhan bisnis;
F. memastikan perolehan dan penggunaan aplikasi atau perangkat lunak hanya bersumber dari penyedia resmi yang dikenal dan memiliki reputasi baik guna mencegah pelanggaran hak cipta;
G. memeriksa kepatuhan penggunaan lisensi aplikasi dan menerapkan pengendalian teknis untuk memastikan jumlah pengguna tidak melampaui batas lisensi yang dimiliki;
H. memelihara dan mengamankan bukti kepemilikan lisensi, master disk atau media instalasi resmi, serta dokumen panduan (*manual book*) terkait;
I. melakukan pemeriksaan secara berkala untuk memastikan tidak adanya penggunaan atau instalasi produk perangkat lunak bajakan (pelanggaran HKI) di lingkungan KP2MI/BP2MI;
J. melakukan reviu secara berkala dan independen terhadap kebijakan, standar, dan implementasi keamanan informasi, serta ketika terjadi perubahan signifikan;
K. mereviu sistem Informasi secara berkala agar sesuai dengan kebijakan dan standar Keamanan Informasi di KP2MI/BP2MI;
L. menyusun, mendokumentasikan, dan memutakhirkan Daftar Risiko (*Risk Register*) serta Rencana Penanganan Risiko (*Risk Treatment Plan*) organisasi secara berkala;
M. melaksanakan penilaian tingkat kematangan penerapan SMKI (Maturity Assessment) dan pengisian instrumen penilaian keamanan secara periodik;
N. menyelenggarakan tinjauan pra-audit (*pre-audit review*) atau penilaian kepatuhan mandiri guna menyusun program kesiapan audit (*audit readiness*), mendampingi dan memfasilitasi kebutuhan Inspektorat Jenderal selaku APIP selama pelaksanaan Audit Internal SMKI, serta mengevaluasi dan memantau penyelesaian tindak lanjut perbaikan (*corrective action*) oleh unit teknis atas setiap temuan dari Bidang Audit Keamanan Informasi; dan

O. segala bentuk pelanggaran terhadap ketentuan SMKI yang mengakibatkan gangguan pada aset informasi akan dikenakan sanksi sesuai dengan peraturan perundang-undangan, kontrak kerja, dan ketentuan internal organisasi.

BAB XVII
AUDIT KEAMANAN INFORMASI

Audit keamanan informasi diselenggarakan secara berkala untuk memastikan kepatuhan dan efektivitas penerapan kebijakan, standar, dan prosedur keamanan informasi yang telah ditetapkan. Pelaksanaan audit keamanan informasi di lingkungan KP2MI/BP2MI terdiri atas Audit Internal dan Audit Eksternal, dengan ketentuan sebagai berikut:

A. Audit Internal Keamanan Informasi:
   1. dilaksanakan oleh Inspektorat Jenderal selaku Aparat Pengawasan Intern Pemerintah (APIP) dengan berkoordinasi bersama Pusat Data dan Informasi selaku pengelola teknis;
   2. dilaksanakan secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun dan dimasukkan ke dalam program kerja pengawasan tahunan serta Peta Rencana SPBE KP2MI/BP2MI;
   3. merencanakan, menyusun, menetapkan, menjadwalkan, dan melaksanakan kegiatan Audit Internal Keamanan Informasi secara objektif dan independen terhadap seluruh penyelenggaraan sistem elektronik;
   4. melibatkan auditor yang memiliki kompetensi memadai, objektivitas, serta imparsialitas (ketidakberpihakan) dalam melaksanakan tugas Audit Internal Keamanan Informasi;
   5. mendokumentasikan dan mencatat setiap temuan audit secara formal oleh auditor untuk disampaikan kepada unit kerja yang diaudit;
   6. melakukan tindakan perbaikan secara tepat oleh unit kerja yang diaudit terhadap setiap temuan hasil audit dalam jangka waktu yang telah disepakati, di bawah pemantauan dan pengawasan Bidang Pengendalian Kepatuhan Tim SMKI;
   7. menyampaikan Laporan Hasil Audit Internal kepada pimpinan instansi dan unit kerja yang diaudit sebagai bahan evaluasi dan perbaikan penerapan Kebijakan SMKI;
   8. menyimpan dan memelihara seluruh dokumen proses serta hasil audit internal sebagai alat bukti pemenuhan program kepatuhan; dan
   9. melaksanakan audit dengan menggunakan instrumen penilaian audit keamanan SPBE yang ditetapkan oleh lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber, atau melalui mekanisme penilaian mandiri (*self-assessment*) menggunakan instrumen yang berlaku secara nasional.

B. Audit Eksternal Keamanan Informasi

   Memanfaatkan hasil Audit Eksternal Keamanan Informasi yang dilaksanakan oleh pihak ketiga sesuai dengan ketentuan peraturan perundang-undangan sebagai dasar peningkatan berkelanjutan terhadap keandalan Sistem Elektronik organisasi.

BAB XVIII
EVALUASI KINERJA DAN PERBAIKAN BERKELANJUTAN KEAMANAN INFORMASI

A. Evaluasi Kinerja Keamanan Informasi

Evaluasi kinerja Keamanan Informasi dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun dalam bentuk tinjauan manajemen untuk memastikan pencapaian target Keamanan Informasi yang telah direncanakan. Sekretaris Jenderal dengan dibantu Tim SMKI melakukan evaluasi kinerja Keamanan Informasi berdasarkan peta rencana, sasaran Keamanan Informasi, dan hasil Audit Keamanan Informasi meliputi:

1. mengidentifikasi area proses yang memiliki Risiko tinggi terhadap keberhasilan pelaksanaan Keamanan Informasi;
2. menetapkan indikator kinerja (*Key Performance Indicators*) pada setiap area proses keamanan informasi;
3. memformulasikan metode pengukuran kinerja secara kuantitatif untuk menilai tingkat keberhasilan pelaksanaan keamanan informasi;
4. melakukan evaluasi terhadap penyelenggaraan atau pelaksanaan SMKI;
5. menganalisis efektivitas pelaksanaan kendali-kendali Keamanan Informasi; dan
6. mendukung dan merealisasikan program Audit Keamanan Informasi sebagai dasar penilaian kepatuhan.

Hasil evaluasi kinerja Keamanan Informasi didokumentasikan untuk digunakan sebagai bahan evaluasi kinerja Keamanan Informasi berikutnya.

B. Perbaikan Berkelanjutan Keamanan Informasi

Perbaikan berkelanjutan merupakan tindak lanjut dari hasil evaluasi kinerja Keamanan Informasi. Tim SMKI melakukan perbaikan berkelanjutan meliputi:

1. mengatasi dan menyelesaikan setiap permasalahan, temuan, atau ketidaksesuaian dalam pelaksanaan Keamanan Informasi; dan
2. memperbaiki dan meningkatkan kualitas pelaksanaan Keamanan Informasi secara berkala mengikuti perkembangan teknologi dan ancaman siber.

Tindakan perbaikan yang telah dilakukan didokumentasikan untuk digunakan sebagai bahan evaluasi kinerja Keamanan Informasi.

Legenda:

Menteri Pelindungan Pekerja Migran Indonesia/ Kepala Badan Pelindungan Pekerja Migran Indonesia	:	Nama jabatan pimpinan Instansi Pemerintah
Sekretaris Jenderal	:	Nama jabatan Sekretaris Instansi Pemerintah
Kepala Pusat Data dan Informasi	:	Nama jabatan setingkat Eselon II yang melaksanakan tugas di bidang keamanan TIK
Tim SMKI	:	Nama Tim / Satuan Tugas Manajemen keamanan informasi
Inspektur Jenderal	:	Nama Unit Kerja / Satuan Kerja yang melaksanakan tugas di bidang audit

BAB XIX
PENUTUP

Sistem Manajemen Keamanan Informasi di KP2MI/BP2MI sebagai pedoman dalam melindungi aset Data dan Informasi di KP2MI/BP2MI dari berbagai bentuk ancaman baik dari dalam maupun luar dengan tujuan untuk menjamin kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan aset Data dan Informasi. Ketentuan mengenai detail operasional teknis dan standar konfigurasi keamanan informasi diatur lebih lanjut melalui Keputusan Kepala Pusat Data dan Informasi, sedangkan struktur organisasi dan keanggotaan Tim SMKI ditetapkan melalui Keputusan Sekretaris Jenderal selaku Ketua Koordinator SPBE.

Dengan disusunnya pedoman ini diharapkan dapat meningkatkan kesadaran seluruh pegawai di lingkungan KP2MI/BP2MI bahwa aset data dan Informasi sangat penting serta menjadi acuan dalam pengamanan data dan Informasi.

MENTERI PELINDUNGAN
PEKERJA MIGRAN INDONESIA/
KEPALA BADAN PELINDUNGAN
PEKERJA MIGRAN INDONESIA
REPUBLIK INDONESIA,

MUKHTARUDIN