



**BADAN PENGAWAS PEMILIHAN UMUM
REPUBLIK INDONESIA**

KEPUTUSAN KETUA BADAN PENGAWAS PEMILIHAN UMUM

NOMOR : 174/TI.01.00/K1/07/2026

TENTANG

**KEBIJAKAN DAN STANDAR SISTEM MANAJEMEN KEAMANAN INFORMASI
BADAN PENGAWAS PEMILIHAN UMUM**

DENGAN RAHMAT TUHAN YANG MAHA ESA

KETUA BADAN PENGAWAS PEMILIHAN UMUM REPUBLIK INDONESIA,

- Menimbang : 1. bahwa untuk menjamin keamanan informasi dalam kerangka sistem pemerintahan berbasis elektronik di lingkungan Badan Pengawas Pemilihan Umum, perlu melaksanakan manajemen keamanan informasi dalam rangka menjamin kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan sumber daya terkait data dan informasi, infrastruktur, dan aplikasi sistem pemerintahan berbasis elektronik;
2. bahwa untuk memberikan pedoman penyelenggaraan keamanan informasi dalam pengelolaan sistem pemerintahan berbasis elektronik di lingkungan Badan Pengawas Pemilihan Umum sesuai dengan ketentuan Pasal 48 Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, Pasal 9 Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik, dan Pasal 22 Peraturan Badan Pengawas Pemilihan Umum Nomor 3 Tahun 2021 tentang Sistem Pemerintahan Berbasis Elektronik, diperlukan pengaturan mengenai manajemen keamanan informasi di lingkungan Badan Pengawas Pemilihan Umum;
3. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Keputusan Ketua Badan Pengawas Pemilihan Umum tentang Kebijakan dan Standar Sistem

- Manajemen Keamanan Informasi Badan Pengawas Pemilihan Umum;
- Mengingat : 1. Undang-Undang Nomor 1 Tahun 2015 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2014 tentang Pemilihan Gubernur, Bupati, dan Walikota menjadi Undang Undang sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 6 Tahun 2020 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2020 tentang Perubahan Ketiga atas Undang-Undang Nomor 1 Tahun 2015 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2014 tentang Pemilihan Gubernur, Bupati, dan Walikota Menjadi Undang-Undang Menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 193, Tambahan Lembaran Negara Republik Indonesia Nomor 6547);
2. Undang-Undang Nomor 7 Tahun 2017 tentang Pemilihan Umum (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 182, Tambahan Lembaran Negara Republik Indonesia Nomor 6109) sebagaimana telah diubah dengan Undang-Undang Nomor 7 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2022 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 2017 tentang Pemilihan Umum Menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 54, Tambahan Lembaran Negara Republik Indonesia Nomor 6863);
3. Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196 dan Tambahan Lembaran Negara Republik Indonesia Nomor 6820);
4. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905);
5. 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);
6. Peraturan Presiden Nomor 68 Tahun 2018 tentang Kedudukan, Tugas, Fungsi, Wewenang, Organisasi, dan Tata Kerja Sekretariat Jenderal Badan Pengawas Pemilihan Umum, Sekretariat Badan Pengawas Pemilihan Umum Provinsi, dan Sekretariat Badan Pengawas Pemilihan Umum Kabupaten/Kota (Lembaran Negara

Republik Indonesia Tahun 2018 Nomor 141);

7. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
8. Peraturan Presiden Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 159);
9. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375);
10. Peraturan Badan Pengawas Pemilihan Umum Nomor 1 Tahun 2021 tentang Organisasi dan Tata Kerja Sekretariat Jenderal Badan Pengawas Pemilihan Umum, Sekretariat Badan Pengawas Pemilihan Umum Provinsi, Sekretariat Badan Pengawas Pemilihan Umum Kabupaten/Kota, dan Sekretariat Panitia Pengawas Pemilihan Umum Kecamatan (Berita Negara Republik Indonesia Tahun 2021 Nomor 411);
11. Peraturan Badan Pengawas Pemilihan Umum Nomor 3 Tahun 2021 tentang Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 1342);
12. 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);
13. Peraturan Badan Pengawas Pemilihan Umum Nomor 3 Tahun 2022 tentang Tata Kerja dan Pola Hubungan Badan Pengawas Pemilihan Umum (Berita Negara Republik Indonesia Tahun 2022 Nomor 889) sebagaimana telah diubah dengan Peraturan Badan Pengawas Pemilihan Umum Nomor 18 Tahun 2023 Tentang Perubahan Atas Peraturan Badan Pengawas Pemilihan Umum Nomor 3 Tahun 2022 Tentang Tata Kerja Dan Pola Hubungan Pengawas Pemilihan Umum (Berita Negara Republik Indonesia Tahun 2023 Nomor 1079);
14. Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2024 tentang Manajemen Keamanan Informasi Siber (Berita Negara Republik Indonesia Tahun 2024 Nomor 44);
15. 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 852);

MEMUTUSKAN:

- Menetapkan : KEPUTUSAN KETUA BADAN PENGAWAS PEMILIHAN UMUM TENTANG KEBIJAKAN DAN STANDAR SISTEM MANAJEMEN KEAMANAN INFORMASI BADAN PENGAWAS PEMILIHAN UMUM.
- KESATU : Menetapkan Kebijakan dan Standar Sistem Manajemen Keamanan Informasi Badan Pengawas Pemilihan Umum sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Keputusan ini.
- KEDUA : Kebijakan dan Standar Sistem Manajemen Keamanan Informasi sebagaimana dimaksud dalam Diktum KESATU menjadi acuan bagi seluruh unit organisasi di lingkungan Badan Pengawas Pemilihan Umum dalam menyelenggarakan Sistem Manajemen Keamanan Informasi sesuai ketentuan peraturan perundang-undangan.
- KETIGA : Unit Organisasi di lingkungan Badan Pengawas Pemilihan Umum melakukan penyesuaian terhadap seluruh aktivitas dan operasional pengelolaan teknologi informasi dan komunikasi dengan ketentuan sebagaimana ditetapkan dalam pedoman ini paling lama 1 (satu) tahun sejak Keputusan ini ditetapkan.
- KEEMPAT : Keputusan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta

pada tanggal 30 Juli 2026

BADAN PENGAWAS PEMILIHAN UMUM

KETUA,



Rahmat Bagja

LAMPIRAN
KEPUTUSAN KETUA BADAN PENGAWAS PEMILIHAN
UMUM REPUBLIK INDONESIA
NOMOR : 174/TI.01.00/K1/07/2026
TANGGAL : 30 Juli 2026
TENTANG
KEBIJAKAN DAN STANDAR SISTEM MANAJEMEN
KEAMANAN INFORMASI BADAN PENGAWAS
PEMILIHAN UMUM

**KEBIJAKAN DAN STANDAR SISTEM MANAJEMEN KEAMANAN INFORMASI
BADAN PENGAWAS PEMILIHAN UMUM**

**BAB I
PENDAHULUAN**

1. Latar Belakang

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik telah mendorong transformasi layanan pemerintahan dari semula dilakukan secara manual menjadi berbasis elektronik atau digital. Transformasi layanan berbasis digital menawarkan berbagai keuntungan antara lain efisiensi, efektivitas, dan akuntabilitas yang tinggi. Namun demikian, transformasi layanan berbasis digital juga menimbulkan risiko baru yaitu munculnya kerentanan dan potensi ancaman terhadap kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan informasi yang dikelola yang diakibatkan oleh berbagai gangguan terhadap sistem yang dimiliki termasuk serangan dan insiden siber.

Keamanan informasi merupakan hal penting yang harus diperhatikan dalam membangun dan menjalankan layanan berbasis digital. Dengan semakin meningkatnya risiko dan insiden siber dalam penyelenggaraan Sistem Pemerintahan Berbasis Elektronik, maka upaya pengamanan terhadap Sistem Pemerintahan Berbasis Elektronik harus dilakukan. Data pribadi, infrastruktur, dan aset lainnya yang dimiliki oleh Badan Pengawas Pemilihan Umum harus dapat dikelola dengan baik. Dalam rangka memberikan perlindungan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan dalam pengelolaan informasi di Badan Pengawas Pemilihan Umum, diperlukan Sistem Manajemen Keamanan Informasi.

Kebijakan Sistem Manajemen Keamanan Informasi disusun sebagai pedoman bagi setiap sumber daya manusia yang terlibat dalam pengelolaan informasi untuk memastikan terjaganya keamanan informasi. Pedoman ini mengatur proses pengelolaan pengamanan informasi maupun kendali yang diperlukan dalam

melakukan pengamanan informasi. Pedoman ini menjadi acuan dalam penyusunan prosedur, petunjuk teknis maupun aturan yang lainnya dalam rangka pengamanan informasi di Badan Pengawas Pemilihan Umum.

2. Maksud dan Tujuan

1. Maksud

Kebijakan dan Standar Sistem Manajemen Keamanan Informasi dimaksudkan untuk memberikan kerangka kerja yang jelas dan terstruktur untuk mengatur, mengelola, dan melindungi informasi yang dimiliki oleh Badan Pengawas Pemilihan Umum.

2. Tujuan

Kebijakan Sistem Manajemen Keamanan Informasi ini digunakan sebagai pedoman dalam rangka melindungi aset informasi Badan Pengawas Pemilihan Umum 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.

3. Sasaran

Sasaran Sistem Manajemen Keamanan Informasi di Badan Pengawas Pemilihan Umum adalah

1. Melindungi informasi sensitif dari akses yang tidak sah, kerusakan, atau perubahan yang tidak sah.
2. Mengidentifikasi dan mengevaluasi risiko terkait dengan keamanan informasi dan mengambil langkah-langkah untuk mengurangi atau mengelola risiko tersebut.
3. Mengelola dan memantau akses ke sistem dan data untuk memastikan hanya orang yang berwenang yang dapat mengakses informasi sensitif.
4. Menyiapkan rencana darurat dan prosedur untuk menangani insiden keamanan, termasuk pelanggaran keamanan dan serangan siber.
5. Melindungi fasilitas fisik dan perangkat keras yang digunakan untuk mengakses dan menyimpan informasi sensitif.
6. Memastikan keamanan pihak ketiga yang memiliki akses ke informasi sensitif atau yang menyediakan layanan yang berkaitan dengan keamanan informasi.
7. Meningkatkan pemahaman dan kesadaran keamanan informasi kepada seluruh pegawai Badan Pengawas Pemilihan Umum.

4. Asas

Kebijakan dan Standar Sistem Manajemen Keamanan Informasi ini disusun berdasarkan asas:

1. Komprehensif, yaitu kebijakan dan standar ini harus mencakup semua aspek keamanan informasi, termasuk kerahasiaan, integritas, dan ketersediaan.
2. Terintegrasi, yaitu kebijakan dan standar ini harus terintegrasi dengan proses bisnis organisasi.
3. Berorientasi pada risiko, yaitu kebijakan dan standar ini harus dirancang untuk mengurangi risiko keamanan informasi.
4. Fleksibel, yaitu kebijakan dan standar ini harus dapat disesuaikan dengan kebutuhan organisasi yang berubah.
5. Efektif, yaitu kebijakan dan standar ini harus efektif dalam melindungi informasi.
6. Kepatuhan, yaitu kebijakan dan standar ini mengacu pada pentingnya mematuhi semua peraturan, undang-undang, dan persyaratan yang berlaku yang berkaitan dengan keamanan informasi.

5. Ruang Lingkup

Kebijakan dan standar ini berlaku untuk pengelolaan pengamanan seluruh aset informasi Badan Pengawas Pemilihan Umum yang dilaksanakan oleh sumber daya manusia yang terlibat baik sebagai pengguna atau pengelola, instansi pemerintah terkait, mitra kerja, dan pihak ketiga di Badan Pengawas Pemilihan Umum. Cakupan aset informasi meliputi:

- a. Data dan Informasi Sistem Pemerintahan Berbasis Elektronik;
- b. Aplikasi Sistem Pemerintahan Berbasis Elektronik;
- c. Infrastruktur Sistem Pemerintahan Berbasis Elektronik; dan
- d. Sumber daya manusia Sistem Pemerintahan Berbasis Elektronik.

6. Pengertian Umum

1. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat 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*, *telecopy* 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, *eletronic data interchange* (EDI),

- surat elektronik (*electronic mail*), telegram, *teleks*, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
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 atau 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. *Risk Treatment Plan* atau Rencana Tindak Lanjut Risiko yang selanjutnya disebut Rencana Tindak Lanjut adalah respon yang direncanakan manajemen untuk menindaklanjuti hasil evaluasi risiko, seperti *mitigate/reduce*, *avoid*, *share/transfer* atau *accept*.
 13. 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. Audit Internal Keamanan Informasi adalah Audit Keamanan Informasi yang dilaksanakan oleh Auditor Keamanan Informasi internal Badan Pengawas Pemilihan Umum
 17. Audit Eksternal Keamanan Informasi adalah Audit Keamanan Informasi yang dilaksanakan oleh Auditor Keamanan Informasi eksternal Badan Pengawas Pemilihan Umum yang memiliki sertifikasi sebagai Auditor Keamanan Informasi.
 18. 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.

19. 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).
20. Tim Tanggap Insiden Siber yang selanjutnya disingkat TTIS adalah sekelompok orang yang bertanggung jawab menangani Insiden Siber dalam ruang lingkup yang ditentukan terhadapnya.
21. 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 Badan Pengawas Pemilihan Umum.

BAB II

ORGANISASI KEAMANAN INFORMASI

1. Umum

Badan Pengawas Pemilihan Umum menetapkan, menerapkan, memelihara, dan memperbaiki secara berkelanjutan SMKI. SMKI dijalankan melalui organisasi keamanan informasi yang peran dan tanggung jawabnya ditetapkan melalui kebijakan dan standar ini.

2. Peran

1. Sekretaris Jenderal selaku Koordinator SPBE berperan sebagai penanggung jawab SMKI.
2. Sekretaris Jenderal dalam menjalankan tugasnya sebagai penanggung jawab SMKI dibantu oleh Tim SMKI selaku pelaksana teknis keamanan informasi.
3. Kepala Pusat Data dan Informasi berperan sebagai Ketua Tim SMKI dan memiliki kewenangan dalam menentukan komposisi, kualifikasi, dan jumlah anggota tim.
4. Tim SMKI ditetapkan oleh Sekretaris Jenderal Badan Pengawas Pemilihan Umum.
5. Sekretaris Jenderal bersama dengan Tim SMKI menjalankan pengelolaan keamanan informasi di Badan Pengawas Pemilihan Umum.
6. Inspektorat Utama berperan melaksanakan Audit Internal Keamanan Informasi.

3. Tanggung Jawab

1. Sekretaris Jenderal bertanggung jawab untuk:
 1. memastikan pelaksanaan Kebijakan SMKI;
 2. menyediakan sumber daya yang memadai untuk menetapkan, mengimplementasikan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan SMKI Badan Pengawas Pemilihan Umum;
 3. menetapkan kriteria penerimaan risiko dan tingkat risiko yang dapat diterima;
 4. memastikan pelaksanaan Audit Internal Keamanan Informasi;
 5. menetapkan arsitektur keamanan informasi;
 6. menetapkan peta rencana 5 (lima) tahunan dan sasaran keamanan informasi setiap tahunnya;
 7. melakukan tinjauan secara berkala atas pelaksanaan kebijakan SMKI; dan
 8. menyampaikan kinerja pelaksanaan kebijakan SMKI kepada Ketua Badan Pengawas Pemilihan Umum;
2. Tim SMKI bertanggung jawab untuk:
 1. menyusun, mengkomunikasikan, dan memantau pelaksanaan kebijakan SMKI di Badan Pengawas Pemilihan Umum;
 2. melakukan analisis kebutuhan keamanan informasi, yang mencakup:
 - 1) mengidentifikasi aplikasi dan infrastruktur untuk keamanan informasi;

- 2) mengidentifikasi standar kompetensi SDM keamanan informasi;
- 3) mengidentifikasi program peningkatan kompetensi keamanan informasi dan penanggulangan insiden siber;
3. merumuskan, mengkoordinasikan, dan melaksanakan program kerja dan anggaran keamanan informasi;
4. memastikan seluruh pembangunan dan/atau pengembangan aplikasi dan infrastruktur informasi 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;
5. memastikan peningkatan kesadaran, kepedulian, dan kepatuhan oleh seluruh pegawai terhadap kebijakan, prosedur, dan standar keamanan informasi;
6. memastikan diterapkannya perjanjian menjaga kerahasiaan aset informasi yang dituangkan dalam dokumen perjanjian kerahasiaan (*Non Disclosure Agreement*);
7. mengendalikan dan menjaga kemutakhiran kebijakan, prosedur, dan standar keamanan informasi;
8. memfasilitasi pelaksanaan audit internal dan audit eksternal keamanan informasi. Dalam memfasilitasi pelaksanaan Audit Internal Keamanan Informasi, Tim SMKI dapat menunjuk pihak yang berkompeten di bidang audit keamanan informasi sebagai konsultan;
9. memastikan diterapkannya manajemen risiko, manajemen insiden siber, dan manajemen aset dalam pelaksanaan pengamanan aset Informasi;
10. mendorong perbaikan penerapan keamanan informasi berdasarkan hasil temuan audit internal dan audit eksternal; dan
11. menyusun laporan evaluasi penerapan Kebijakan SMKI dan menyampaikannya kepada Sekretaris Jenderal.
3. Inspektorat Utama bertanggung jawab untuk:
 1. menyusun pedoman pelaksanaan Audit Internal Keamanan Informasi di lingkungan Badan Pengawas Pemilihan Umum sesuai dengan ketentuan peraturan perundang-undangan;
 2. menyusun perencanaan Audit Internal Keamanan Informasi;
 3. melaksanakan kegiatan Audit Internal Keamanan Informasi;
 4. memberikan rekomendasi perbaikan atas hasil temuan Audit Internal Keamanan Informasi;
 5. menyusun laporan Audit Internal Keamanan Informasi; dan
 6. menyampaikan laporan Audit Internal Keamanan Informasi kepada Sekretaris Jenderal.

BAB III

PERENCANAAN KEAMANAN INFORMASI

1. Kategorisasi Sistem Elektronik

Badan Pengawas Pemilihan Umum sebagai Penyelenggara SPBE yang merupakan Sistem Elektronik Lingkup Publik, melakukan kategorisasi setiap sistem elektronik yang dimilikinya sebagai salah satu dasar dalam pelaksanaan keamanan informasi. Penentuan kategorisasi sistem elektronik dilakukan sesuai dengan peraturan perundangan yang ditetapkan oleh Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

2. Manajemen Risiko

Pelaksanaan keamanan informasi dilakukan dengan memperhatikan berbagai risiko yang dapat mengakibatkan terjadinya kegagalan keamanan informasi di Badan Pengawas Pemilihan Umum. Oleh karenanya, dalam melakukan perencanaan keamanan informasi, Tim SMKI melakukan manajemen risiko keamanan informasi, yang terdiri dari:

1. menyusun penilaian risiko keamanan informasi dengan mengidentifikasi ancaman, kerentanan, peluang, dan dampak apabila risiko terjadi;
2. bersama dengan unit terkait, menyusun Rencana Tindak Lanjut (RTL);
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.

3. 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;
2. penilaian kerentanan keamanan informasi;
3. peningkatan 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 sasaran keamanan informasi yang ditetapkan untuk setiap tahunnya. Peta rencana keamanan informasi sebagaimana dimaksud menjadi bagian dari peta rencana SPBE.

BAB IV

DUKUNGAN PENGOPERASIAN

1. Sekretaris Jenderal memberikan dukungan pengoperasian keamanan informasi dengan menyediakan SDM keamanan informasi yang berkompeten dan anggaran keamanan informasi.
2. SDM keamanan informasi yang disediakan harus memiliki kompetensi:
 1. Keamanan Infrastruktur TIK;
 2. Keamanan Aplikasi; dan
 3. Keamanan Data.
3. Dalam hal SDM keamanan informasi yang disediakan belum memiliki kompetensi memadai, maka Sekretaris Jenderal memfasilitasi peningkatan kompetensi melalui kegiatan pelatihan dan/atau bimbingan teknis.
4. Memfasilitasi penyelenggaraan kegiatan kesadaran keamanan informasi bagi pegawai di lingkungan Badan Pengawas Pemilihan Umum.
5. Sekretaris Jenderal menyediakan anggaran keamanan informasi berdasarkan arsitektur dan peta rencana keamanan informasi yang telah disusun.
6. Anggaran keamanan informasi dibebankan pada DIPA Badan Pengawas Pemilihan Umum atau sumber lainnya yang sah dan tidak mengikat.

BAB V

KENDALI KEAMANAN

1. KEAMANAN SDM

Keamanan SDM dilakukan untuk mengendalikan SDM dalam melaksanakan Kebijakan SMKI. Keamanan SDM di Badan Pengawas Pemilihan Umum dilaksanakan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. mengkomunikasikan peran dan tanggung jawab pelaksanaan Kebijakan SMKI kepada seluruh pegawai dan pihak ketiga yang terlibat dalam pengelolaan dan pengamanan aset informasi;
2. melakukan pembagian tugas dan wewenang (*segregation of duty*) untuk menghindari kesalahan atau pelanggaran;
3. melakukan pengelolaan sumber daya manusia sebelum status kepegawaian dimulai dan selama status kepegawaian berjalan atau selama bekerja di lingkungan Badan Pengawas Pemilihan Umum;
4. melakukan pemeriksaan data pribadi pegawai dan pihak ketiga yang terlibat dalam pengelolaan dan pengamanan aset informasi;
5. membuat perjanjian tertulis dengan pegawai dan pihak ketiga yang terlibat dalam penggunaan dan/atau pengelolaan informasi yang menyatakan tanggung jawab terhadap keamanan informasi dan sanksi atas pelanggaran keamanan informasi;
6. menghentikan hak penggunaan aset informasi bagi pegawai yang sedang dalam pemeriksaan terkait dengan dugaan pelanggaran keamanan informasi;
7. mencabut hak akses ke aset informasi yang dimiliki pegawai dan pihak ketiga apabila yang bersangkutan tidak lagi memiliki kepentingan terhadap aset informasi, dimutasi, atau tidak lagi bekerja di Badan Pengawas Pemilihan Umum;
8. membuat berita acara serah terima terkait penerimaan seluruh aset informasi yang dipergunakan selama bekerja dan pengembalian seluruh aset informasi bagi pegawai yang berhenti bekerja atau mutasi;
9. memberikan edukasi kesadaran keamanan informasi melalui kegiatan sosialisasi, bimbingan teknis, dan/atau pelatihan mengenai keamanan informasi yang dilaksanakan secara berkala;
10. memelihara catatan pelatihan, kompetensi, pengalaman, dan kualifikasi pegawai yang mengelola keamanan informasi; dan
11. melaksanakan simulasi ancaman keamanan informasi (seperti *phishing simulation* atau *social engineering*) minimal 1 (satu) kali dalam setahun untuk meningkatkan kesadaran keamanan siber.

2. KEAMANAN ASET INFORMASI

Keamanan aset informasi dilakukan untuk mengamankan aset informasi di Badan Pengawas Pemilihan Umum berdasarkan tingkat kritikalitasnya. Keamanan aset informasi di Badan Pengawas Pemilihan Umum dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. mengidentifikasi dan mengklasifikasikan aset informasi serta dan mendokumentasikannya dalam daftar inventaris aset informasi yang memuat tingkat kritikalitas dan penanggung jawab setiap aset;
2. memberikan label sesuai tingkat kritikalitas;
3. menetapkan pihak-pihak yang dapat mengakses aset informasi;
4. menetapkan aturan penggunaan aset informasi;
5. menempatkan aset informasi di lokasi yang aman guna mengurangi risiko aset informasi dapat diakses oleh pihak yang tidak berwenang;
6. penggunaan aset yang dibawa ke luar dari lingkungan Pusat Data atau tempat layanan informasi harus disetujui oleh Kepala Pusat Data dan Informasi;
7. perangkat penyimpanan data yang sudah tidak digunakan lagi harus disanitasi sebelum digunakan kembali atau dimusnahkan;
8. pemusnahan perangkat penyimpanan data harus dilakukan secara aman sesuai Prosedur Pemusnahan Perangkat Penyimpanan; dan
9. melaksanakan manajemen aset TIK sesuai dengan ketentuan manajemen aset TIK yang ditetapkan oleh Kementerian yang melaksanakan tugas di bidang Komunikasi dan Digital.
10. mengatur penggunaan perangkat pribadi (*smartphone*, laptop, media penyimpanan) yang digunakan untuk mengakses aset informasi dengan ketentuan:
 1. Setiap perangkat pribadi yang digunakan wajib memiliki standar keamanan minimum seperti penggunaan PIN atau Biometrik, sistem operasi yang *terupdate*, dan bebas dari aplikasi berbahaya.
 2. Pengguna bertanggung jawab penuh atas keamanan data pribadi dan data kedinasan yang diakses melalui perangkat tersebut.
 3. Tim SMKI berwenang melakukan penghapusan data kedinasan secara jarak jauh (*remote wipe*) jika perangkat pribadi hilang atau personel berhenti bertugas.
11. mengatur pemisahan antara data pribadi dan data kedinasan pada perangkat yang digunakan untuk bekerja guna mencegah kebocoran data sensitif atau data pribadi;

3. KEAMANAN AKSES

Keamanan akses dilakukan untuk mengendalikan akses ke aset informasi yaitu memastikan perangkat pengguna yang terhubung ke aset informasi mendapatkan perlindungan keamanan dan tidak diakses oleh pihak yang tidak berhak. Keamanan akses terhadap aset informasi di Badan Pengawas Pemilihan Umum dilakukan oleh Tim

SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. menyusun Prosedur Pengelolaan Hak Akses Pengguna yang berisi ketentuan akses ke aset informasi sesuai dengan kebutuhan organisasi, persyaratan keamanan, dan peraturan yang berlaku;
2. mengelola akses pengguna dengan cara:
 1. menggunakan akun yang unik untuk setiap pengguna;
 2. memeriksa tingkat akses yang diberikan sesuai dengan tujuan penggunaan;
 3. membatasi dan mengendalikan penggunaan hak akses khusus (jika ada);
 4. mengatur pengelolaan kata sandi pengguna sesuai dengan Ketentuan Pengelolaan Kata Sandi di Badan Pengawas Pemilihan Umum;
 5. memantau dan mengevaluasi hak akses pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya;
 6. memelihara catatan pengguna layanan (*user log*) dan membuat laporan secara berkala;
 7. menonaktifkan akses pengguna yang telah berakhir penugasannya; dan
 8. memantau dan mengevaluasi akun dan hak akses secara berkala paling sedikit 1 (satu) kali dalam 6 (enam) bulan.
3. mengendalikan akses ke jaringan dan layanan jaringan informasi dengan cara;
 1. menerapkan Prosedur Otorisasi Pemberian Akses ke Jaringan dan Layanan Jaringan untuk setiap akses ke dalam jaringan internal;
 2. akses ke infrastruktur dan aplikasi yang digunakan untuk melakukan diagnosa harus dikontrol dan hanya digunakan untuk pegawai yang bertugas untuk melakukan pengujian, pemecahan masalah, serta pengembangan sistem;
 3. memisahkan jaringan untuk pengguna, sistem informasi, dan layanan informasi;
 4. memberikan akses jaringan kepada tamu hanya untuk akses terbatas dan waktu tertentu; dan
 5. melakukan penghentian layanan jaringan pada area jaringan yang mengalami gangguan keamanan informasi.
4. mengendalikan akses ke aplikasi dan sistem informasi dengan cara;
 1. akses terhadap aplikasi dan sistem informasi hanya diberikan kepada pengguna melalui mekanisme administrasi formal yang dibuktikan dengan *form* permohonan, *form* perpanjangan, serta *form* pencabutan hak akses sesuai dengan peruntukannya dan dikontrol dengan menggunakan sistem manajemen akses pengguna;
 2. setiap pengguna wajib memiliki akun yang unik dan hanya digunakan sesuai dengan peruntukannya dan proses otorisasi pengguna wajib menggunakan teknik otentikasi yang sesuai untuk memvalidasi identitas pengguna;

3. menggunakan sistem pengelolaan kata sandi sesuai dengan Ketentuan Pengelolaan Kata Sandi di Badan Pengawas Pemilihan Umum untuk memastikan kualitas kata sandi yang dibuat pengguna;
4. fasilitas *session time-out* wajib diaktifkan untuk menutup dan mengunci layar komputer, aplikasi, dan koneksi jaringan apabila tidak ada aktivitas pengguna setelah periode tertentu;
5. membatasi waktu koneksi untuk sistem informasi dan aplikasi yang memiliki klasifikasi rahasia dan/atau sangat rahasia; dan
6. akses ke kode sumber aplikasi dibatasi secara ketat diperuntukkan hanya bagi pihak-pihak yang sah dan berkepentingan melalui hak akses khusus.
5. mengendalikan perangkat kerja jarak jauh dengan cara menentukan parameter-parameter keamanan yang harus dipenuhi oleh perangkat kerja jarak jauh yang digunakan dalam mengakses aset informasi, yang terdiri dari namun tidak terbatas pada:
 1. *Virtual Private Network* (VPN);
 2. *Secure Socket Layer* (SSL); dan/atau
 3. *Multi Factor Authentication*;
6. hak akses khusus dapat dibuat untuk mengakses sistem informasi berklasifikasi rahasia pada sistem operasi, perangkat penyimpanan (*storage devices*), *file server*, dan aplikasi sensitif, dengan cara:
 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 catatan dari seluruh hak akses khusus; dan
 4. memberikan hak akses khusus secara terpisah dari akun yang digunakan untuk kegiatan lainnya.
7. melakukan pemantauan terhadap akses ke aset informasi 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.
8. menghapus akun setiap pegawai dan pihak ketiga yang tidak lagi memiliki kepentingan terhadap akses aset informasi, dimutasi, berhenti, atau telah berakhir kontraknya; dan
9. penggunaan perangkat pribadi untuk mengakses aset informasi wajib mendapatkan otorisasi tertulis melalui Surat Izin Penggunaan Perangkat Pribadi dan memenuhi standar keamanan yang ditetapkan.

4. KEAMANAN KRIPTOGRAFI

Keamanan kriptografi untuk memastikan penggunaan kriptografi yang tepat untuk melindungi kerahasiaan, keutuhan, dan keotentikan data dan informasi rahasia dan/atau sangat rahasia yang dikelola dalam perangkat informasi. Keamanan kriptografi untuk informasi rahasia dan/atau sangat rahasia dilaksanakan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. melakukan klasifikasi informasi yang disimpan dan dikelola dalam perangkat informasi sesuai dengan peraturan yang berlaku.
2. menerapkan keamanan kriptografi untuk informasi berklasifikasi rahasia dan/atau sangat rahasia dengan cara sebagai berikut namun tidak terbatas pada:
 1. menerapkan jalur komunikasi aman dengan menerapkan *Secure Socket Layer* (SSL) untuk proses otentikasi 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 dipertukarkirinkan dan disimpan dalam basis data dengan melakukan enkripsi;
 4. menerapkan otentikasi berbasis tanda tangan digital dengan menggunakan sertifikat elektronik yang dikeluarkan oleh Pihak Ketiga Terpercaya; 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 melakukan peninjauan algoritma secara berkala.

5. KEAMANAN FISIK DAN LINGKUNGAN

Keamanan fisik dan lingkungan dilakukan untuk memberikan perlindungan, pemeliharaan, keamanan, dan ketersediaan aset informasi. Keamanan fisik dan lingkungan dilaksanakan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. Menyimpan infrastruktur di ruangan khusus yang dilindungi dengan pengamanan fisik yang memadai antara lain namun tidak terbatas pada:
 1. Pintu dengan kontrol akses;
 2. Kamera pengawas (CCTV);
 3. Pendeteksi asap;
 4. Sistem pemadam kebakaran; dan
 5. Perangkat pemutus aliran listrik.
2. Akses ke Pusat Data dan/atau area kerja layanan informasi yang berisi data dan/atau informasi rahasia dan/atau sangat rahasia harus dibatasi dan hanya diberikan kepada pegawai yang memiliki akses;

3. Pihak Ketiga yang memasuki Pusat Data dan/atau area kerja layanan informasi yang berisikan data dan/atau informasi rahasia dan/ atau sangat rahasia harus didampingi oleh pegawai yang ditugaskan sepanjang waktu kunjungan;
4. Makanan dan minuman dilarang untuk dibawa masuk dan/atau dikonsumsi di dalam ruang *server* Pusat Data;
5. Semua area yang digunakan untuk menyimpan aset informasi merupakan area bebas rokok;
6. Batas minimum dan maksimum suhu dan kelembaban di dalam ruang *server* Pusat Data harus memenuhi standar yang disyaratkan pabrikan perangkat dan senantiasa dilakukan pengawasan terhadap kondisi suhu dan kelembaban dengan *log* pencatatan harian guna menjamin usia pakai perangkat;
7. Pengamanan area Pusat Data dan area kerja layanan informasi dilakukan sesuai Prosedur Keamanan Area dengan menerapkan zonasi keamanan untuk membatasi akses personel berdasarkan kepentingan;
8. Pengamanan kantor, ruangan, dan fasilitas kerja sesuai dengan peraturan dan standar keamanan dan keselamatan kerja, termasuk *clear screen policy* dan *clean desk policy*;
9. Infrastruktur yang digunakan untuk menjalankan aplikasi dipelihara sesuai dengan buku petunjuk;
10. Dalam hal pemeliharaan infrastruktur tidak dapat dilakukan di tempat, maka pemindahan infrastruktur dilakukan berdasarkan persetujuan Kepala Pusat Data dan Informasi;
11. Dalam hal pemindahan infrastruktur terdapat data dan/atau informasi berklasifikasi rahasia dan/atau sangat rahasia yang tersimpan pada perangkat tersebut, maka data dan/atau informasi berklasifikasi rahasia dan/atau sangat rahasia tersebut harus dipindahkan terlebih dahulu ke dalam media penyimpanan lain;
12. Dalam hal pemeliharaan dilakukan oleh Pihak Ketiga, maka pelaksanaannya dilakukan dengan membuat perjanjian kerja sama yang paling sedikit memuat perjanjian menjaga kerahasiaan, pemeliharaan yang disediakan, dan tingkat kinerja yang harus dipenuhi Pihak Ketiga;
13. Infrastruktur beserta perangkat pemulihan dan media penyimpanan data cadangan wajib diletakkan di tempat yang aman dengan struktur yang memadai untuk menghindari kerusakan dari hama (misal: tikus, semut dan rayap) dan bencana (misal: banjir dan gempa);
14. Semua infrastruktur harus mendapatkan pasokan daya yang sesuai dengan spesifikasi yang diisyaratkan oleh pabrikan infrastruktur;
15. Pasokan listrik yang digunakan untuk mengoperasikan infrastruktur harus mempunyai sumber alternatif dengan daya dan jangka waktu ketersediaan atau jangka waktu pengoperasian yang cukup, yang paling sedikit mencakup generator listrik dan *Uninterruptable Power Supply* (UPS) dengan daya yang cukup dan

dengan konfigurasi yang dapat memindahkan pasokan listrik tanpa gangguan terhadap infrastruktur;

16. Bahan berbahaya atau mudah terbakar di lingkungan Badan Pengawas Pemilihan Umum wajib disimpan pada jarak yang aman dari Pusat Data dan area kerja layanan informasi;
17. Perangkat pemadam kebakaran wajib disediakan, dipelihara, dan diletakkan di tempat yang mudah dijangkau;
18. Infrastruktur diletakkan pada lokasi yang meminimalisasi akses pihak yang tidak berwenang;
19. infrastruktur yang menangani informasi sensitif diposisikan dan dibatasi sudut pandangnya untuk mengurangi risiko informasi dilihat oleh pihak tidak berwenang;
20. perlindungan petir harus diterapkan untuk semua bangunan, jalur komunikasi dan listrik;
21. pengamanan kabel di Pusat Data dan/atau area kerja layanan informasi dilakukan dengan mengikuti standar mekanikal atau elektrikal Pusat Data yang berlaku;
22. melaksanakan inspeksi kelayakan ruang *server* secara berkala yang mencakup ketahanan material bangunan, sistem proteksi kebakaran, dan deteksi kebocoran; dan
23. memastikan tersedianya *log* kendali perangkat yang terdiri dari detail waktu, personel, dan tujuan atas setiap aktivitas pemindahan infrastruktur dari maupun menuju ruang *server*.

6. KEAMANAN OPERASIONAL

Keamanan operasional dilakukan untuk memastikan implementasi, operasional, dan pemeliharaan yang aman dari aset informasi, pengelolaan layanan oleh Pihak Ketiga, meminimalkan risiko kegagalan, dan melindungi keutuhan dan ketersediaan aset informasi. Keamanan operasional di Badan Pengawas Pemilihan Umum dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait, cara sebagai berikut namun tidak terbatas pada:

1. mendokumentasikan, memelihara, dan menyediakan Prosedur Penggunaan Perangkat Informasi sesuai dengan peruntukannya;
2. perubahan pada aset informasi yang dapat mempengaruhi keamanan informasi harus didokumentasikan dan dikendalikan dengan memperhatikan manajemen risiko dan persetujuan dari pemilik aset informasi;
3. menetapkan kriteria penerimaan untuk sistem informasi baru, pemutakhiran dan versi baru serta melakukan pengujian sebelum penerimaan;
4. memantau penggunaan aset informasi yang dimiliki dan membuat proyeksi kebutuhan ke depan untuk menjamin ketersediaan aset informasi yang dibutuhkan. Untuk aset informasi yang kritis harus senantiasa dimonitor dan dievaluasi kapasitas dan ketersediaannya;

5. 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);
6. memisahkan lingkungan pengembangan, pengujian, dan operasional untuk mengurangi risiko perubahan atau akses oleh pihak yang tidak berhak terhadap sistem operasional;
7. menerapkan sistem pendeteksian, pencegahan, dan pemulihan sebagai bentuk perlindungan terhadap ancaman *malware*;
8. Perlindungan dilakukan dengan cara pemasangan paling sedikit meliputi:
 1. perangkat *firewall*;
 2. perangkat *Intrusion Detection System* (IDS);
 3. perangkat *Intrusion Prevention System* (IPS);
 4. perangkat antivirus;
 5. perangkat manajemen akses pengguna; dan
 6. perangkat monitoring atau pendukung lainnya sesuai perkembangan teknologi keamanan informasi.
9. melakukan pembuatan *backup* informasi dan aplikasi yang berada di Pusat Data dan/atau area kerja layanan informasi secara berkala sesuai dengan Prosedur *Backup* di Badan Pengawas Pemilihan Umum dengan melakukan pencadangan minimal 3 salinan data, pada 2 media berbeda, dengan 1 salinan berada di lokasi geografis berbeda;
10. salinan cadangan data/informasi, aplikasi, dan *image* sistem harus diambil dan diuji secara berkala dengan melakukan simulasi pemulihan data dari media cadangan minimal setiap 6 (enam) bulan untuk memastikan kesiapan sistem pasca-bencana;
11. mencatat (*logging*) setiap aktivitas administrator, aktivitas pengguna, peristiwa kegagalan, dan kejadian keamanan serta disimpan dalam periode tertentu;
12. melindungi sistem pencatatan (*log*) dari pemalsuan dan akses yang tidak berwenang;
13. melakukan penilaian kerentanan terhadap perangkat informasi (*vulnerability assessment*) secara berkala dan melakukan tindakan perlindungan terhadap kerentanan dan/atau ancaman yang teridentifikasi;
14. menerapkan pencatatan kesalahan untuk dianalisis dan diambil tindak pengamanan yang tepat;
15. memastikan semua perangkat pengolah informasi yang tersambung dengan jaringan telah disinkronisasi dengan sumber waktu yang akurat dan disepakati;
16. menerapkan audit terhadap *log* yang mencatat aktivitas pengguna dan kejadian keamanan informasi dalam kurun waktu tertentu untuk membantu investigasi di masa mendatang, antara lain:
 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.
17. mengelola konfigurasi perangkat secara terpusat dan terdokumentasi untuk meminimalisir perubahan yang tidak terotorisasi;
 18. menerapkan prosedur Manajemen Perubahan yang mencakup pencatatan, pengujian, dan persetujuan atas setiap perubahan konfigurasi pada infrastruktur dan aplikasi;
 19. menetapkan daftar perangkat lunak yang diizinkan (*Whitelist Software*) dan standar versi sistem operasi yang boleh digunakan pada perangkat *desktop* maupun *server*; dan
 20. mengatur penggunaan *add-on*, *plugin*, dan ekstensi pada *web browser* pada perangkat BMN dengan ketentuan:
 1. hanya diperbolehkan menggunakan *add-on* atau *plugin* yang telah diverifikasi keamanannya dan memiliki reputasi resmi dari penyedia aplikasi;
 2. dilarang memasang ekstensi yang meminta hak akses berlebihan terhadap data sensitif atau kredensial pengguna tanpa alasan teknis yang jelas; dan
 3. melakukan peninjauan dan pembersihan berkala terhadap daftar *add-on* yang terpasang untuk memastikan tidak ada komponen yang bersifat berbahaya atau tidak digunakan lagi.

7. KEAMANAN KOMUNIKASI

Keamanan komunikasi dilakukan untuk memastikan keamanan pertukaran informasi melalui jaringan komunikasi. Keamanan komunikasi di Badan Pengawas Pemilihan Umum dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. Tim SMKI mengidentifikasi fitur keamanan layanan, tingkat layanan, dan kebutuhan pengelolaan dalam kesepakatan penyediaan layanan jaringan termasuk layanan jaringan yang disediakan oleh Pihak Ketiga;
2. dalam hal Pihak Ketiga diizinkan mengakses ke jaringan, maka dilakukan pemantauan serta pencatatan kegiatan selama menggunakan jaringan; dan
3. melindungi jaringan dari pihak yang tidak berhak mengakses, paling sedikit dengan cara:
 1. mendokumentasikan arsitektur jaringan yang meliputi seluruh komponen infrastruktur dan aplikasi jaringan;
 2. menerapkan teknologi keamanan jaringan berbasis enkripsi dan otentikasi (termasuk sertifikat elektronik);
 3. menerapkan pemisahan jaringan untuk kelompok pengguna, layanan informasi, dan sistem informasi;

4. menerapkan parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan; dan
 5. menerapkan Prosedur Penggunaan Layanan Jaringan yang membatasi akses ke layanan jaringan atau aplikasi.
4. menerapkan mekanisme kriptografi untuk melindungi informasi yang terdapat dalam aplikasi yang melewati jaringan publik dari upaya pengungkapan, modifikasi, dan perusakan;
 5. melakukan pendeteksian dan perlindungan terhadap kode berbahaya (*malicious code*) yang disisipkan pada file yang dikirim melalui sistem elektronik;
 6. memberikan perlindungan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan untuk informasi elektronik berklasifikasi rahasia dan/atau sangat rahasia;
 7. menetapkan Prosedur Pertukaran informasi yang mengatur sistem dan keamanan yang digunakan untuk pertukaran informasi;
 8. mengimplementasikan protokol pengamanan *email* untuk mencegah upaya pemalsuan identitas (*spoofing*), *phishing*, dan penyebaran *malware* melalui *email*, yang meliputi:
 1. SPF (*Sender Policy Framework*);
 2. DKIM (*DomainKeys Identified Mail*);
 3. DMARC (*Domain-based Message Authentication, Reporting, and Conformance*);
 4. *Email Sandboxing*.
 9. melakukan sosialisasi secara berkala kepada seluruh pengguna *email* resmi kedinasan mengenai cara mengidentifikasi email mencurigakan meskipun telah melewati filter keamanan teknis; dan
 10. menerapkan *Web Application Firewall* (WAF) yang dilengkapi dengan fitur *IP Reputation* untuk memblokir akses dari alamat *IP* yang teridentifikasi berbahaya atau memiliki rekam jejak aktivitas ilegal.

8. KEAMANAN PENGEMBANGAN DAN PEMELIHARAAN

Keamanan pengembangan dan pemeliharaan sistem dilakukan untuk memastikan bahwa keamanan informasi merupakan bagian yang terintegrasi dalam daur hidup aset informasi untuk mencegah terjadinya kesalahan, eksploitasi, modifikasi, dan perusakan aset informasi oleh pihak yang tidak berwenang. Keamanan pengembangan dan pemeliharaan di Badan Pengawas Pemilihan Umum dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. lingkungan pengembangan, pengujian, dan operasional aplikasi harus dipisahkan baik secara fisik, *logic*, maupun aksesnya;
2. menjaga agar lingkungan pengembangan tidak boleh diakses dari sistem operasional layanan;

3. mengupayakan lingkungan pengujian sama dengan lingkungan operasional layanan;
4. memilih data uji dengan hati-hati, melindungi, dan mengendalikannya;
5. mengawasi dan memantau aktivitas pembangunan atau pengembangan aplikasi dan infrastruktur yang dialihdayakan pada pihak ketiga;
6. memastikan bahwa dalam proses perencanaan dan pembangunan/pengembangan aplikasi dan infrastruktur termasuk yang dilakukan oleh Pihak Ketiga, telah memasukkan fitur-fitur keamanan dalam spesifikasi aplikasi dan infrastruktur yang dibangun/dikembangkan;
7. fitur-fitur keamanan yang dimasukkan sesuai dengan standar keamanan relevan, yang mencakup:
 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.
8. standar keamanan sebagaimana dimaksud pada angka 7 (tujuh) minimal memenuhi standar keamanan yang ditetapkan oleh Lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber.
9. melaksanakan uji kelaikan aplikasi sebelum aplikasi digunakan dan sewaktu-waktu sesuai kebutuhan, yang mencakup aspek:
 1. uji fungsi, dilakukan untuk memastikan aplikasi yang dibangun dan/atau dikembangkan telah memenuhi fungsi-fungsi sesuai dengan dokumentasi terkait;
 2. uji integrasi, 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, dilakukan untuk yang memastikan aplikasi yang dibangun dan/atau dikembangkan dapat berfungsi sebagaimana mestinya menghadapi beban kerja yang dikenakan terhadapnya;
 4. uji keamanan, dilakukan untuk memastikan aplikasi yang dibangun dan/atau dikembangkan dapat menjaga keamanan data dan informasi yang terkait dengannya.
10. uji kelaikan pada aspek uji fungsi, uji integrasi, dan uji beban dapat menggunakan pedoman/instrumen pengukuran yang ditetapkan oleh Kementerian yang menyelenggarakan tugas pemerintahan di bidang komunikasi dan digital;
11. uji kelaikan pada aspek uji keamanan dapat menggunakan pedoman atau instrumen pengukuran yang ditetapkan oleh Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber;

12. pelaksanaan pembangunan dan pengembangan aplikasi dilakukan sesuai dengan Standar Teknis dan Prosedur Pembangunan dan Pengembangan Aplikasi yang ditetapkan oleh Kementerian yang melaksanakan tugas di bidang Komunikasi dan Digital; dan
13. mengelola seluruh *source code* aplikasi menggunakan *version control system* serta melaksanakan *source code review* secara berkala atau sebelum rilis aplikasi untuk mendeteksi adanya celah keamanan teknis, kesalahan logika, maupun *malicious code*.

9. KEAMANAN PIHAK KETIGA

Keamanan Pihak Ketiga dilakukan untuk memastikan perlindungan dari aset informasi yang dapat diakses oleh Pihak Ketiga. Keamanan Pihak Ketiga di Badan Pengawas Pemilihan Umum dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. melakukan pemeriksaan latar belakang Pihak Ketiga dengan tetap memperhatikan privasi dan perlindungan data pribadi;
2. membuat dan meninjau ulang secara berkala perjanjian keamanan dengan pihak ketiga yang terlibat dalam penggunaan dan/atau pengelolaan aset informasi yang menyatakan tanggung jawab terhadap keamanan aset informasi. Perjanjian keamanan sebagaimana dimaksud dibuat secara tertulis paling sedikit memuat:
 1. perlindungan atas informasi rahasia dan/atau sangat rahasia dan hak kekayaan intelektual setiap pihak;
 2. dalam hal aset informasi disediakan oleh Pihak Ketiga, maka adanya jaminan bahwa tidak terdapat *malicious code* dan *backdoor*;
 3. hak untuk melakukan audit dan memantau kegiatan yang melibatkan informasi rahasia dan/atau sangat rahasia;
 4. pengawasan atas akses terhadap aset informasi yang diberikan pada pihak ketiga;
 5. pelaporan terhadap penyingkapan yang dilakukan secara tidak sah atau pelanggaran terhadap kerahasiaan;
 6. syarat untuk informasi yang akan dikembalikan atau dimusnahkan pada saat penghentian perjanjian;
 7. penggunaan jalur komunikasi yang aman untuk perpindahan informasi antara Badan Pengawas Pemilihan Umum dengan pihak ketiga; dan
 8. dalam hal Pihak Ketiga tidak lagi menjadi bagian dalam pengelolaan aset informasi, maka aset informasi yang dikuasainya diserahkan kembali kepada Tim SMKI.
3. 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;

4. memastikan *Service Level Agreement* (SLA) pihak ketiga telah mengatur ketersediaan layanan dan penyelesaian insiden keamanan;
5. melakukan pemantauan terhadap kinerja penyediaan layanan, laporan, dan catatan yang disediakan oleh Pihak Ketiga secara berkala;
6. memperhatikan kritikalitas, proses yang terkait dan hasil penilaian ulang risiko layanan apabila terjadi perubahan pada layanan yang disediakan oleh Pihak Ketiga;
7. mencatat peristiwa keamanan, masalah operasional, kegagalan, dan gangguan yang terkait dengan layanan yang diberikan oleh pihak ketiga;
8. memberikan informasi tentang gangguan keamanan dan mengkaji informasi bersama Pihak Ketiga;
9. mencabut hak akses terhadap akses informasi yang dimiliki Pihak Ketiga apabila yang bersangkutan tidak lagi bekerja di Badan Pengawas Pemilihan Umum;
10. membuat berita acara serah terima terkait mengembalikan seluruh aset informasi yang dipergunakan selama bekerja bagi Pihak Ketiga yang berakhir masa kontraknya;
11. memastikan Pihak Ketiga dan tamu yang memasuki lingkungan Pusat Data, dan tempat layanan informasi harus mematuhi standar keamanan fisik dan lingkungan; dan
12. memastikan Pihak Ketiga untuk mengisi dan menyerahkan *Checklist* Pemenuhan Standar Keamanan secara berkala sebagai verifikasi atas kepatuhan mereka terhadap SMKI.

10. MANAJEMEN INSIDEN SIBER

Manajemen insiden siber dilaksanakan untuk mengendalikan insiden siber. Manajemen insiden siber di Badan Pengawas Pemilihan Umum dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. membentuk Tim Tanggap Insiden siber (TTIS) yang bertugas melakukan pencegahan dan penanganan insiden siber yang terjadi di Badan Pengawas Pemilihan Umum;
2. Tim Tanggap Insiden siber melakukan tindakan pencegahan insiden siber paling sedikit meliputi:
 1. melakukan penilaian kerentanan dan/atau *penetration testing* untuk menemukan celah keamanan pada aset informasi;
 2. mengimplementasikan alat monitoring keamanan berupa *Security Information and Event Management* (SIEM); dan
 3. melakukan monitoring dan pendeteksian serangan terhadap aset informasi.
3. Dalam hal terjadi insiden siber, Tim Tanggap Insiden siber melaksanakan Prosedur Penanganan Insiden siber paling sedikit meliputi:
 1. menerima laporan dan mencatat insiden siber;

2. melakukan triase insiden siber;
 3. mengidentifikasi sumber serangan;
 4. menganalisis informasi yang berkaitan dengan insiden siber;
 5. memprioritaskan penanganan insiden berdasarkan tingkat dampak;
 6. memelihara artefak digital untuk keperluan investigasi;
 7. menyusun laporan penanganan insiden siber; dan
 8. mengevaluasi dan memperbaiki standar, prosedur, dan kontrol-kontrol keamanan informasi agar insiden siber serupa tidak terulang kembali di masa mendatang.
4. menyusun berbagai macam skenario penanganan insiden siber;
 5. melakukan simulasi secara berkala skenario penanganan insiden siber yang telah disusun;
 6. memberikan pelatihan terhadap SDM yang terlibat pada penanganan insiden siber sesuai skenario yang disusun;
 7. menjalankan program kesadaran ancaman dan penanganan insiden siber, serta ajakan peran aktif pada seluruh pegawai;
 8. memastikan tersedianya kontak pelaporan insiden siber yang dapat diakses oleh seluruh pegawai di Badan Pengawas Pemilihan Umum termasuk oleh pihak ketiga;
 9. melakukan pengukuran tingkat kematangan penanganan insiden siber secara berkala; dan
 10. mengidentifikasi dan menetapkan kriteria kejadian gangguan keamanan informasi yang wajib dilaporkan dan ditindaklanjuti oleh TTIS, yang mencakup namun tidak terbatas pada:
 1. Tidak efektifnya kontrol atau kendali keamanan informasi yang telah ditetapkan;
 2. Kegagalan fungsi, kerusakan, atau beban berlebih (*overload*) pada sistem informasi;
 3. Kesalahan manusia (*human error*) dalam pengoperasian aset informasi;
 4. Ketidakpatuhan (*non-compliance*) terhadap kebijakan dan prosedur keamanan yang berlaku;
 5. Pelanggaran atau tembusnya pengamanan fisik dan lingkungan;
 6. Pelaksanaan perubahan sistem atau konfigurasi yang tidak terkendali;
 7. Kegagalan fungsi perangkat lunak maupun perangkat keras; dan
 8. Pelanggaran hak akses atau penggunaan akun yang tidak sah.

11. MANAJEMEN KEBERLANGSUNGAN LAYANAN INFORMASI

Manajemen keberlangsungan layanan informasi dilakukan untuk menjamin ketersediaan layanan informasi pada saat terjadi keadaan darurat. Manajemen keberlangsungan layanan informasi dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. melakukan identifikasi risiko terhadap keberlangsungan layanan informasi;
2. menyusun dan menerapkan rencana keberlangsungan layanan informasi (*Business Continuity Planning*) untuk menjaga dan mengembalikan operasional aset informasi dalam jangka waktu yang disepakati dan tingkat keberlangsungan yang dibutuhkan;
3. rencana keberlangsungan layanan informasi paling sedikit meliputi:
 1. 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. penetapan peran dan penanggung jawab pegawai yang terlibat dalam pelaksanaan keberlangsungan layanan informasi;
 3. pelaksanaan sosialisasi dan pelatihan keberlangsungan layanan informasi;
4. jika aplikasi merupakan aplikasi umum atau sistem elektronik berkategori strategis, maka harus memiliki redundansi yang cukup untuk memenuhi ketersediaan layanan informasi;
5. melakukan uji coba rencana keberlangsungan layanan informasi secara berkala; dan
6. pelaksanaan pengelolaan layanan dilakukan sesuai dengan pedoman manajemen layanan SPBE yang ditetapkan oleh Kementerian yang melaksanakan tugas di bidang Komunikasi dan Informatika.

12. PENGENDALIAN KEPATUHAN

Pengendalian kepatuhan dilaksanakan untuk memastikan kepatuhan pegawai dan Pihak Ketiga dalam melaksanakan keamanan informasi sesuai dengan ketentuan peraturan perundang-undangan, kontrak dan keselarasan dengan kebijakan keamanan informasi yang berlaku di Badan Pengawas Pemilihan Umum. Pengendalian kepatuhan keamanan informasi di Badan Pengawas Pemilihan Umum, dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. mengidentifikasi, mendokumentasikan, mereviu, dan memelihara regulasi, standar, dan prosedur keamanan informasi;
2. memeriksa kepatuhan seluruh pegawai dan Pihak Ketiga terhadap regulasi, standar, dan prosedur keamanan informasi;
3. mendapatkan aplikasi hanya melalui sumber yang dikenal dan memiliki reputasi baik untuk memastikan tidak ada pelanggaran hak cipta;
4. memeriksa kepatuhan penggunaan lisensi aplikasi secara berkala (minimal 1 tahun sekali) dan menerapkan pengendalian untuk memastikan jumlah pengguna tidak melampaui lisensi yang dimiliki;

5. Memastikan seluruh perangkat lunak yang berlisensi mendapatkan pembaruan keamanan (*security patch*) secara rutin guna menutup celah keamanan;
6. memelihara bukti kepemilikan lisensi, *master disk*, buku panduan, dan lain sebagainya;
7. melakukan pemeriksaan bahwa tidak ada produk bajakan yang terinstal (pelanggaran hak kekayaan intelektual) di Badan Pengawas Pemilihan Umum;
8. memastikan rekaman terlindungi dari kehilangan, kerusakan, pemalsuan, akses tidak sah, dan rilis tidak sah sesuai dengan persyaratan peraturan perundang-undangan, kontraktual, dan bisnis;
9. memastikan pengamanan privasi dan data pribadi yang dapat diidentifikasi sesuai dengan persyaratan peraturan perundang-undangan yang berlaku;
10. memastikan tersedianya mekanisme formal bagi subjek data untuk melaksanakan haknya seperti permintaan akses atau koreksi data sesuai dengan regulasi yang berlaku;
11. melakukan klasifikasi jenis pelanggaran keamanan informasi (ringan, sedang, berat) dan menetapkan eskalasi sanksi bagi pegawai yang terbukti melakukan pelanggaran kebijakan atau kelalaian dalam perlindungan data pribadi (*insider threat*).
12. memastikan kesesuaian penerapan kriptografi dengan peraturan perundang-undangan yang berlaku; dan
13. melakukan reviu sistem informasi secara berkala agar sesuai dengan kebijakan dan standar keamanan informasi di Badan Pengawas Pemilihan Umum.

13. KEAMANAN DATA PRIBADI

Keamanan Data Pribadi dilaksanakan untuk menjamin perlindungan hak-hak subjek data dan memastikan kepatuhan pegawai dan Pihak Ketiga terhadap regulasi perlindungan data pribadi. Keamanan Data Pribadi di Badan Pengawas Pemilihan Umum, dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. menerapkan Kebijakan Privasi (*Privacy Policy*) dan Persetujuan Pengguna (*Consent*) pada setiap layanan digital Badan Pengawas Pemilihan Umum yang melakukan pemrosesan data pribadi;
2. menyusun dan memelihara Peta Alur Data (*Data Flow Diagram*) yang menggambarkan siklus hidup data pribadi mulai dari perolehan, pemrosesan, penyimpanan, hingga penghapusan;
3. menerapkan prinsip *Privacy by Design* dan *Privacy by Default* dalam setiap pengembangan aplikasi atau sistem informasi baru;
4. menerapkan teknik pengaburan data seperti *Data Masking* atau Data Sensor pada tampilan informasi publik maupun internal untuk data yang bersifat sensitif sesuai dengan ketentuan peraturan Bawaslu;

5. menerapkan enkripsi pada penyimpanan (*at rest*) dan pengiriman (*in transit*) untuk data pribadi yang bersifat spesifik;
6. menerapkan mekanisme *Data Loss Prevention* (DLP) pada sistem komunikasi untuk mencegah pengiriman data pribadi keluar dari lingkungan internal tanpa otorisasi;
7. menyediakan mekanisme penghapusan atau pemusnahan data pribadi (hak untuk dilupakan) berdasarkan permintaan pemilik data yang sah sesuai dengan ketentuan peraturan perundang-undangan;
8. melaksanakan Penilaian Dampak Perlindungan Data (*Data Protection Impact Assessment*) secara berkala terhadap sistem yang memiliki risiko tinggi pada subjek data;
9. menetapkan prosedur notifikasi kegagalan data pribadi yang mewajibkan penyampaian pemberitahuan tertulis kepada subjek data dan lembaga otoritas dalam waktu paling lambat 3 x 24 jam sejak terjadinya insiden; dan
10. melakukan audit kepatuhan perlindungan data pribadi secara mandiri atau melalui pihak ketiga untuk memastikan seluruh proses bisnis di lingkungan Badan Pengawas Pemilihan Umum selaras dengan mandat UU PDP.

BAB VI

AUDIT KEAMANAN INFORMASI

Audit keamanan informasi dilaksanakan secara berkala untuk memastikan diterapkannya kebijakan, standar, dan prosedur keamanan informasi. Audit keamanan informasi dilaksanakan melalui kegiatan Audit Internal Keamanan Informasi dan Audit Eksternal keamanan informasi yang dilaksanakan dengan cara sebagai berikut namun tidak terbatas pada:

1. Audit Internal Keamanan Informasi

1. Audit Internal Keamanan Informasi di Badan Pengawas Pemilihan Umum dilaksanakan oleh Inspektorat Utama;
2. Inspektorat Utama merencanakan, menetapkan, dan menjalankan program audit sesuai dengan pedoman Audit Internal Keamanan Informasi;
3. Program audit minimal mencakup frekuensi, metode, kriteria, lingkup, tanggung jawab, dan pelaporan audit, serta mempertimbangkan pentingnya proses yang sedang berjalan dan hasil audit sebelumnya;
4. Audit Internal Keamanan Informasi dilaksanakan paling sedikit 1 (satu) kali dalam 2 (dua) tahun dan dimasukkan dalam Peta Rencana SPBE Badan Pengawas Pemilihan Umum;
5. Audit Internal Keamanan Informasi dilaksanakan oleh Auditor yang memiliki kompetensi memadai dan memiliki objektivitas serta imparialitas (ketidakberpihakan) dalam melaksanakan Audit Internal Keamanan Informasi;
6. Setiap temuan audit harus dicatat secara formal oleh Auditor dan diberikan kepada auditan;
7. Auditan harus melakukan perbaikan terhadap setiap temuan yang diberikan oleh Auditor dalam jangka waktu yang disepakati;
8. Laporan Hasil Audit Keamanan Informasi dilaporkan kepada Tim SMKI dan Sekretaris Jenderal sebagai bahan evaluasi penerapan Kebijakan SMKI;
9. Menyimpan dan mendokumentasikan proses dan hasil audit internal sebagai alat bukti dari program audit; dan
10. Pelaksanaan Audit Internal Keamanan Informasi dapat menggunakan instrumen penilaian Audit Keamanan SPBE yang ditetapkan oleh Kepala Lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber.

2. Audit Eksternal Keamanan Informasi

Audit Eksternal Keamanan Informasi di Badan Pengawas Pemilihan Umum dilaksanakan oleh Pihak Ketiga sesuai dengan peraturan perundang-undangan yang berlaku.

BAB VII

EVALUASI KINERJA DAN PERBAIKAN BERKELANJUTAN KEAMANAN INFORMASI

1. Evaluasi Kinerja

Untuk memastikan pelaksanaan sistem manajemen keamanan informasi terlaksana sesuai dengan ketentuan yang berlaku, maka perlu dilakukan pelaksanaan Evaluasi sistem manajemen 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 dengan cara sebagai berikut namun tidak terbatas pada:

1. mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan keamanan informasi;
2. menetapkan indikator kinerja pada setiap area proses;
3. memformulasi pelaksanaan keamanan informasi dengan mengukur secara kuantitatif kinerja yang diharapkan;
4. melakukan evaluasi terhadap penyelenggaraan atau pelaksanaan SMKI termasuk jika ada perubahan yang terkait dengan rencana SMKI atau Bisnis Proses yang ada;
5. menganalisis efektifitas pelaksanaan keamanan informasi; dan
6. mendukung dan merealisasikan program Audit Keamanan Informasi.

Hasil evaluasi kinerja keamanan informasi didokumentasikan untuk digunakan sebagai bahan evaluasi kinerja keamanan informasi berikutnya.

2. Perbaikan Berkelanjutan Keamanan Informasi

Perbaikan berkelanjutan merupakan tindak lanjut dari hasil evaluasi kinerja keamanan informasi. Tim SMKI melakukan perbaikan berkelanjutan dengan cara sekurang-kurangnya sebagai berikut:

1. mengatasi permasalahan dalam pelaksanaan keamanan informasi;
2. memperbaiki pelaksanaan keamanan informasi secara berkala.

Tindakan perbaikan yang telah dilakukan didokumentasikan untuk digunakan sebagai bahan evaluasi kinerja keamanan informasi.

BAB VIII

PENUTUP

Kebijakan dan Standar Sistem Keamanan Manajemen Informasi Badan Pengawas Pemilihan Umum ini ditetapkan sebagai acuan dalam merancang, mengimplementasikan, mengoperasikan, dan memelihara Sistem Manajemen Keamanan Informasi Sistem Pemerintah Berbasis Elektronik di lingkungan Badan Pengawas Pemilihan Umum.

BADAN PENGAWAS PEMILIHAN UMUM

KETUA,



Rahmat Bagja