SALINAN

MENTERI DESA, PEMBANGUNAN DAERAH TERTINGGAL, DAN TRANSMIGRASI REPUBLIK INDONESIA

KEPUTUSAN MENTERI
DESA, PEMBANGUNAN DAERAH TERTINGGAL, DAN TRANSMIGRASI
REPUBLIK INDONESIA

NOMOR 55 TAHUN 2023

TENTANG

KEBIJAKAN DAN STANDAR SISTEM MANAJEMEN KEAMANAN INFORMASI KEMENTERIAN DESA, PEMBANGUNAN DAERAH TERTINGGAL, DAN TRANSMIGRASI

MENTERI DESA, PEMBANGUNAN DAERAH TERTINGGAL, DAN TRANSMIGRASI REPUBLIK INDONESIA,

Menimbang :

a. bahwa dalam rangka melindungi kerahasiaan, keutuhan, dan ketersediaan aset informasi Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi dari berbagai bentuk ancaman keamanan informasi baik dari dalam maupun luar, perlu menyusun kebijakan dan standar sistem manajemen keamanan informasi;

b. bahwa guna mewujudkan pengelolaan keamanan aset informasi Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi perlu dibangun sistem manajemen keamanan informasi yang selaras dengan Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengembangan Informasi;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Keputusan Menteri Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi tentang Kebijakan dan Standar Sistem Manajemen Keamanan Informasi Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi;

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. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Nomor 182);
3. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112);
4. Peraturan Presiden Nomor 85 Tahun 2020 tentang Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 192);
5. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);
6. Peraturan Menteri Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi Nomor 22 Tahun 2019 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi Republik Indonesia (Berita Negara Republik Indonesia Tahun 2019 Nomor 1753);
7. Peraturan Menteri Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi Nomor 15 Tahun 2020 tentang Organisasi dan Tata Kerja Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi (Berita Negara Republik Indonesia Tahun 2020 Nomor 1256) sebagaimana telah diubah dengan Peraturan Menteri Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi Nomor 5 Tahun 2022 tentang Perubahan atas Peraturan Menteri Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi Nomor 15 Tahun 2020 tentang Organisasi dan Tata Kerja Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi (Berita Negara Republik Indonesia Tahun 2022 Nomor 823);
8. 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);

Memperhatikan : ISO/IEC 270001:2013 *(Information Technology – Security Techniques – Information Security Management System-Requirements);*

MEMUTUSKAN:

Menetapkan : KEPUTUSAN MENTERI DESA, PEMBANGUNAN DAERAH TERTINGGAL, DAN TRANSMIGRASI TENTANG KEBIJAKAN DAN STANDAR SISTEM MANAJEMEN KEAMANAN INFORMASI KEMENTERIAN DESA, PEMBANGUNAN DAERAH TERTINGGAL, DAN TRANSMIGRASI.

KESATU : Menetapkan kebijakan dan standar sistem manajemen keamanan informasi Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Keputusan Menteri ini.

KEDUA : Kebijakan dan Standar Sistem Manajemen Keamanan Informasi Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi sebagaimana dimaksud dalam Diktum KESATU digunakan sebagai pedoman atau standar dalam rangka melindungi aset informasi Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi dari berbagai bentuk ancaman baik dari dalam maupun dari luar lingkungan Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi, dengan tujuan untuk menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi.

KETIGA : Keputusan Menteri ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 24 Maret 2023

MENTERI DESA,
PEMBANGUNAN DAERAH TERTINGGAL, DAN TRANSMIGRASI
REPUBLIK INDONESIA,

ttd.

ABDUL HALIM ISKANDAR

Salinan sesuai aslinya
Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi
Plt. Kepala Biro Hukum

Rully Rachman

LAMPIRAN
KEPUTUSAN MENTERI DESA, PEMBANGUNAN DAERAH TERTINGGAL, DAN TRANSMIGRASI
REPUBLIK INDONESIA
NOMOR 55 TAHUN 2023
TENTANG
KEBIJAKAN DAN STANDAR SISTEM MANAJEMEN KEAMANAN INFORMASI KEMENTERIAN DESA, PEMBANGUNAN DAERAH TERTINGGAL, DAN TRANSMIGRASI

KEBIJAKAN DAN STANDAR SISTEM MANAJEMEN KEAMANAN INFORMASI KEMENTERIAN DESA, PEMBANGUNAN DAERAH TERTINGGAL, DAN TRANSMIGRASI

SISTEMATIKA

BAB I
PENDAHULUAN

A. PENDAHULUAN

Dalam rangka memberikan perlindungan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan dalam pengelolaan keamanan informasi di lingkungan Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi, maka diperlukan Kebijakan dan Standar Sistem Manajemen Keamanan Informasi. Kebijakan dan Standar Sistem Manajemen Keamanan Informasi ini disusun sebagai pedoman bagi setiap personil yang terlibat dalam pengelolaan keamanan informasi untuk memastikan terjaganya keamanan informasi selama proses pembangunan / pengembangan, operasional, dan pemusnahan informasi.

Kebijakan dan Standar Sistem Manajemen Keamanan Informasi digunakan sebagai acuan dalam rangka melindungi aset informasi Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi dari berbagai bentuk ancaman baik dari dalam maupun dari luar, yang dilakukan secara sengaja maupun tidak sengaja. Pengamanan dan perlindungan ini diberikan untuk menjamin tiga (3) komponen utama yang menjadi dasar keamanan informasi, yaitu aspek kerahasiaan *(Confidentiality),* keutuhan *(Integrity),* dan ketersediaan *(Availability)* atau CIA pada aset informasi agar selalu terjaga dan terpelihara dengan baik.

Informasi yang berada dalam berbagai bentuk (tersimpan pada sistem komputer, ditransmisikan melalui jaringan komunikasi tercetak dalam bentuk *hardcopy* atau diucapkan dalam pembicaraan), harus diamankan dengan cara yang tepat agar ketiga aspek CIA tersebut selalu terjaga.

B. MAKSUD DAN TUJUAN

Kebijakan dan Standar Sistem Manajemen Keamanan Informasi menyatakan komitmen dan arahan Manajemen untuk melaksanakan prinsip-prinsip keamanan informasi. Kebijakan dan Standar Sistem Manajemen Keamanan Informasi disusun dengan tujuan agar dapat:

1. Memastikan terpeliharanya kerahasiaan, integritas, dan ketersediaan informasi Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi, serta seluruh sistem sumber daya informasi;

2. Membangun pengamanan untuk melindungi aset informasi milik Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi dari ancaman pencurian, penyalahgunaan, atau kerusakan;
3. Memastikan terlaksananya prinsip *non-repudiation* atas pihak-pihak yang terlibat dalam proses bisnis Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi;
4. Menetapkan tanggung jawab dan akuntabilitas penggunaan dalam mengakses informasi milik Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi;
5. Memastikan terpenuhinya kepatuhan terhadap hukum, undang-undang, dan peraturan eksternal yang berlaku;
6. Memastikan kemampuan Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi untuk melanjutkan aktivitasnya dalam hal terjadi insiden keamanan informasi yang signifikan atau ancaman terhadap sistem informasi Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi;
7. Mendorong manajemen dan seluruh pegawai Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi untuk memiliki tingkat kesadaran *(awareness),* pengetahuan dan keterampilan yang memadai agar dapat memenuhi kewajiban mereka dalam menjaga keamanan aset informasi;
8. Memiliki sumber daya yang memadai untuk melaksanakan program keamanan informasi yang efektif; dan
9. Memastikan konsistensi dalam menerapkan keamanan informasi.

C. RUANG LINGKUP

Ruang lingkup Keamanan Informasi yaitu melindungi, kerahasiaan, keutuhan, ketersediaan, otentikasi, dan kenirsangkalan aset informasi dalam bentuk:

a. data dan informasi;
b. perangkat lunak; dan
c. perangkat keras

D. ORGANISASI KEAMANAN INFORMASI DI LINGKUNGAN KEMENTERIAN DESA, PEMBANGUNAN DAERAH TERTINGGAL, DAN TRANSMIGRASI

1. Kepala Badan Pengembangan dan Informasi Desa, Daerah Tertinggal, dan Transmigrasi selaku Koordinator SPBE bertanggungjawab atas pelaksanaan Kebijakan Keamanan Informasi.
2. Kepala Badan Pengembangan dan Informasi Desa, Daerah Tertinggal, dan Transmigrasi dalam menjalankan tugasnya sebagai Koordinator SPBE dibantu oleh Pusat Data dan Informasi Pembangunan Desa, Daerah Tertinggal, dan Transmigrasi selaku Pelaksana Teknis Keamanan Informasi.
3. Pelaksana Teknis Keamanan Informasi beranggotakan Kepala Pusat Data dan Informasi Pembangunan Desa, Daerah Tertinggal, dan Transmigrasi dan Computer Security Incident Response Team (CSIRT) di lingkungan Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi.
4. Kepala Badan Pengembangan dan Informasi Desa, Daerah Tertinggal, dan Transmigrasi bersama dengan Pelaksana Teknis Keamanan Informasi menjalankan tata kelola keamanan informasi di lingkungan Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi.
5. Tata kelola keamanan informasi dijalankan melalui kepastian standar dan prosedur untuk memberikan jaminan pengelolaan kebijakan keamanan informasi.

BAB II
PENGENDALIAN KEAMANAN INFORMASI

A. TANGGUNG JAWAB

Koordinator SPBE bertanggung jawab untuk:

1. memastikan pelaksanaan Kebijakan Keamanan Informasi;
2. memberikan dukungan pengoperasian yang dibutuhkan dalam pelaksanaan Kebijakan Keamanan Informasi; dan
3. membuat peta rencana dan target keamanan informasi setiap tahunnya.

Pelaksana Teknis Keamanan Informasi bertanggung jawab untuk:

1. memastikan Kebijakan Keamanan Informasi dilaksanakan secara efektif oleh para pihak terkait;
2. melakukan analisis kebutuhan keamanan informasi, mencakup:
   a. mengidentifikasi perangkat lunak dan perangkat keras untuk keamanan informasi;
   b. mengidentifikasi standar kompetensi / keahlian personil pengelola keamanan informasi;
   c. mengidentifikasi program peningkatan kompetensi keamanan informasi; dan
   d. mengidentifikasi program peningkatan kemampuan penanggulangan insiden keamanan siber;
3. mengendalikan dan menjaga kemutakhiran kebijakan, prosedur, dan standar Keamanan Informasi;
4. memastikan peningkatan kesadaran, kepedulian, dan kepatuhan oleh seluruh pegawai terhadap kebijakan, prosedur, dan standar Keamanan Informasi;
5. memastikan diterapkannya perjanjian menjaga kerahasiaan aset informasi yang dituangkan dalam dokumen perjanjian kerahasiaan (*Non Disclosure Agreement*);
6. memfasilitasi pelaksanaan audit internal dan audit eksternal Keamanan Informasi. Dalam memfasilitasi pelaksanaan audit internal Keamanan Informasi, Pelaksana Teknis Keamanan Informasi dapat

menunjuk pihak yang berkompeten di bidang audit teknologi informasi sebagai konsultan;

7. mendorong perbaikan penerapan Keamanan Informasi dan tindak lanjut temuan auditor eksternal;
8. membuat laporan evaluasi penerapan Kebijakan Keamanan Informasi dan menyampaikannya kepada Kepala Badan Pengembangan dan Informasi Desa, Daerah Tertinggal, dan Transmigrasi.

Pusat Data dan Informasi Pembangunan Desa, Daerah Tertinggal, dan Transmigrasi bertanggung jawab untuk:

1. merumuskan, mengkoordinasikan, dan melaksanakan program kerja dan anggaran keamanan informasi;
2. mengawasi penerapan kebijakan, prosedur, dan standar Keamanan Informasi;
3. menetapkan prosedur-prosedur yang terkait dengan penggunaan, pemeliharaan, dan keamanan informasi;
4. mengidentifikasi dan menetapkan penanggung jawab setiap aset informasi;
5. meningkatkan pengetahuan, keterampilan, dan kepedulian keamanan informasi pada seluruh pengguna informasi;
6. menerapkan prinsip manajemen risiko dalam pelaksanaan pengamanan dan perlindungan aset informasi; dan
7. menindaklanjuti laporan hasil audit internal dan audit eksternal Keamanan Informasi.

Tim Kerja yang menangani Teknologi Informasi dan Komunikasi bertanggung jawab untuk:

1. menjalankan kebijakan, prosedur, dan standar Keamanan Informasi untuk pengamanan aset informasi;
2. memastikan seluruh pembangunan / pengembangan aplikasi dan infrastruktur SPBE termasuk yang dilakukan oleh Pihak Ketiga, memenuhi Standar Teknis dan Prosedur Keamanan SPBE yang ditetapkan oleh Lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber;
3. menyusun **Prosedur Penggunaan Aset Informasi**;

4. memantau, mencatat, menguraikan, dan menindaklanjuti gangguan keamanan informasi yang diketahui atau dilaporkan sesuai **Prosedur Penanganan Gangguan Keamanan Informasi**;
5. melaksanakan identifikasi dan pengklasifikasian aset informasi berdasarkan tingkat risiko serta mendokumentasikan ke dalam daftar inventaris aset informasi;
6. menempatkan dokumen keamanan informasi (Prosedur, Formulir, Instruksi Kerja) pada semua area operasional agar mudah diakses sesuai dengan peruntukannya; dan
7. melaksanakan penyelesaian masalah keamanan informasi.

Pegawai di lingkungan Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi selaku pengguna informasi bertanggung jawab untuk:

1. menjaga keamanan aset informasi dalam penggunaannya sesuai dengan kebijakan, prosedur, dan standar keamanan informasi; dan
2. menandatangani pakta integritas yang diwakilkan oleh Unit Eselon II.

B. DUKUNGAN PENGOPERASIAN

1. Kepala Badan Pengembangan dan Informasi Desa, Daerah Tertinggal, dan Transmigrasi memberikan dukungan pengoperasian keamanan informasi dengan menyediakan personil keamanan informasi yang berkompeten dan anggaran keamanan informasi.
2. Personil keamanan informasi yang disediakan harus memiliki kompetensi:
    a. Keamanan Infrastruktur TIK; dan
    b. Keamanan Aplikasi.
3. Dalam hal personil keamanan informasi yang disediakan belum memiliki kompetensi memadai, maka Kepala Badan Pengembangan dan Informasi Desa, Daerah Tertinggal, dan Transmigrasi memfasilitasi peningkatan kompetensi melalui kegiatan pelatihan dan/atau bimbingan teknis.
4. Kepala Badan Pengembangan dan Informasi Desa, Daerah Tertinggal, dan Transmigrasi menyediakan anggaran keamanan informasi berdasarkan peta rencana keamanan informasi yang telah disusun.

5. Anggaran Keamanan informasi dibebankan pada Anggaran Pendapatan dan Belanja Negara atau sumber lainnya yang sah dan tidak mengikat.

C. KEAMANAN PERSONIL

Keamanan Personil dilakukan untuk mengendalikan Personil dalam melaksanakan kebijakan keamanan informasi. Keamanan Personil di lingkungan Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi dilaksanakan oleh Kepala Badan Pengembangan dan Informasi Desa, Daerah Tertinggal, dan Transmigrasi bersama dengan Pelaksana Teknis Keamanan Informasi dengan cara sebagai berikut:

1. mengkomunikasikan peran dan tanggung jawab pelaksanaan Kebijakan Keamanan informasi kepada Kepala Pusat Data dan Informasi Pembangunan Desa, Daerah Tertinggal, Tim CSIRT, dan pegawai yang terlibat dalam pengelolaan dan pengamanan aset informasi;
2. membuat perjanjian tertulis dengan pegawai yang terlibat dalam penggunaan dan/atau pengelolaan informasi yang menyatakan tanggung jawab terhadap keamanan informasi dan sanksi atas pelanggaran keamanan informasi;
3. menghentikan hak penggunaan aset informasi bagi pegawai yang sedang dalam pemeriksaan terkait dengan dugaan pelanggaran Keamanan informasi;
4. mencabut hak akses ke aset informasi yang dimiliki pegawai apabila yang bersangkutan tidak lagi memiliki kepentingan terhadap aset informasi, dimutasi atau tidak lagi bekerja di lingkungan Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi;
5. membuat berita acara serah terima terkait mengembalikan seluruh aset informasi yang dipergunakan selama bekerja bagi pegawai yang berhenti bekerja atau mutasi; dan
6. memberikan edukasi kesadaran keamanan informasi melalui kegiatan sosialisasi, bimbingan teknis, dan pelatihan mengenai keamanan sistem informasi yang dilaksanakan secara berkala sesuai dengan tingkat tanggung jawabnya.

D. KEAMANAN ASET

Keamanan aset dilakukan untuk mengamankan aset informasi di lingkungan Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi berdasarkan tingkat kritikalitasnya. Aset terdiri dari data dan informasi, perangkat lunak, dan perangkat keras. Keamanan aset informasi di lingkungan Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi dilakukan oleh Pusat Data dan Informasi Pembangunan Desa, Daerah Tertinggal, dan Transmigrasi dengan cara sebagai berikut:

1. mengidentifikasi aset informasi dan mendokumentasikannya dalam daftar inventaris aset informasi yang juga memuat tingkat kritikalitas dan penanggungjawab setiap aset;
2. menetapkan pihak-pihak yang dapat mengakses aset informasi;
3. menetapkan aturan penggunaan aset informasi;
4. mengidentifikasi potensi ancaman dan penilaian tingkat risiko *(risk register)* keamanan 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 pimpinan Pusat Data dan Informasi Pembangunan Desa, Daerah Tertinggal, dan Transmigrasi;
7. Perangkat penyimpanan data yang sudah tidak digunakan lagi harus disanitasi sebelum digunakan kembali atau dimusnahkan; dan
8. Pemusnahan perangkat penyimpanan data harus dilakukan secara aman sesuai Prosedur Pemusnahan Perangkat Penyimpanan.

E. 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 lingkungan Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi dilakukan oleh Pusat Data dan Informasi Pembangunan Desa, Daerah Tertinggal, dan Transmigrasi dengan cara sebagai berikut:

1. menyusun Prosedur Pengelolaan Hak Akses Pengguna yang berisi ketentuan akses ke aset informasi sesuai dengan kebutuhan organisasi dan persyaratan keamanannya;
2. mengelola akses pengguna dengan cara:
    a. menggunakan akun yang unik untuk setiap pengguna;
    b. memeriksa tingkat akses yang diberikan sesuai dengan tujuan penggunaan;
    c. membatasi dan mengendalikan penggunaan hak akses khusus (jika ada);
    d. mengatur pengelolaan kata sandi pengguna;
    e. memantau dan mengevaluasi hak akses pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya;
    f. memelihara catatan pengguna layanan (user log);
    g. menonaktifan akses pengguna yang telah berakhir penugasannya; dan
    h. memeriksa dan menonaktifan akun secara berkala.
3. mengendalikan akses ke jaringan dan layanan jaringan informasi dengan cara:
    a. menerapkan Prosedur Otorisasi Pemberian Akses Ke Jaringan Dan Layanan Jaringan untuk setiap akses ke dalam jaringan internal;
    b. akses ke perangkat keras dan perangkat lunak yang digunakan untuk melakukan diagnosa harus dikontrol dan hanya digunakan untuk pegawai yang bertugas untuk melakukan pengujian, pemecahan masalah, serta pengembangan sistem;
    c. memisahkan jaringan untuk pengguna, sistem informasi, dan layanan informasi;
    d. memberikan akses jaringan kepada tamu hanya untuk akses terbatas dan waktu tertentu; dan
    e. melakukan penghentian layanan jaringan pada area jaringan yang mengalami gangguan keamanan informasi.
4. mengendalikan akses ke aplikasi dan sistem informasi informasi dengan cara:
    a. akses terhadap aplikasi informasi hanya diberikan kepada pengguna sesuai dengan peruntukannya dan dikontrol dengan menggunakan sistem manajemen akses pengguna;

b. 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;
c. menggunakan sistem pengelolaan password yang dapat memastikan kualitas password yang dibuat pengguna;
d. fasilitas session time-out wajib diaktifkan untuk menutup dan mengunci layar komputer, aplikasi, dan koneksi jaringan apabila tidak ada aktivitas pengguna setelah periode tertentu; dan
e. membatasi waktu koneksi untuk sistem informasi dan aplikasi yang memiliki klasifikasi rahasia dan sangat rahasia.
f. 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 sesuai dengan cara menentukan parameter-parameter keamanan yang harus dipenuhi oleh perangkat kerja jarak jauh yang digunakan dalam mengakses aset informasi, yang dapat terdiri dari namun tidak terbatas pada:
   a. *Virtual Private Network* (VPN);
   b. *Secure Socket Layer* (SSL); dan/atau
   c. *Two Step 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:
   a. mengidentifikasi hak akses khusus untuk dialokasikan kepada pengguna terkait;
   b. memberikan hak akses khusus hanya kepada pengguna sesuai dengan peruntukannya berdasarkan kebutuhan dan kegiatan tertentu;
   c. mengelola proses otorisasi dan catatan dari seluruh hak akses khusus; dan
   d. memberikan hak akses khusus secara terpisah dari akun yang digunakan untuk kegiatan umum.
7. melakukan pemantauan terhadap akses ke aset informasi meliputi:
   a. kegagalan akses;
   b. penggunaan hak akses tidak wajar;
   c. alokasi dan penggunaan hak akses khusus;

d. penelusuran transaksi pengiriman file sistem atau dokumen tertentu yang mencurigakan; dan
e. 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.

F. 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 pengolah informasi. Keamanan kriptografi untuk informasi rahasia dan/atau sangat rahasia dilaksanakan oleh Pusat Data dan Informasi Pembangunan Desa, Daerah Tertinggal, dan Transmigrasi dengan cara sebagai berikut:

1. melakukan klasifikasi informasi yang disimpan dan dikelola dalam perangkat pengolah informasi sesuai dengan regulasi yang berlaku.
2. menerapkan keamanan kriptografi untuk informasi berklasifikasi rahasia dan/atau sangat rahasia dengan cara sebagai berikut:
    a. menerapkan jalur komunikasi aman dengan menerapkan *Secure Socket Layer* (SSL) untuk proses otentikasi antara pengguna dengan perangkat informasi berbasis website;
    b. menjaga kerahasiaan password dan menyimpannya dalam database informasi dengan mekanisme *hash function*;
    c. melindungi kerahasiaan data dan informasi rahasia dan/atau sangat rahasia dalam database informasi dengan mekanisme kriptografi simetrik;
    d. menerapkan otentikasi berbasis tanda tangan digital dengan menggunakan sertifikat elektronik yang dikeluarkan oleh Pihak Ketiga Terpercaya; dan
    e. menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan peraturan perundangan dan/atau rekomendasi Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

G. KEAMANAN FISIK DAN LINGKUNGAN

Keamanan fisik dan lingkungan dilakukan untuk memberikan pelindungan, pemeliharaan, dan keamanan perangkat pengolah informasi. Keamanan fisik dan lingkungan dilaksanakan oleh Pusat Data dan Informasi Pembangunan Desa, Daerah Tertinggal, dan Transmigrasi dengan cara sebagai berikut:

1. pemeliharaan perangkat pengolah informasi;
2. pengamanan area;
3. perlindungan terhadap ancaman eksternal dan lingkungan;
4. penempatan dan perlindungan perangkat; dan
5. pengamanan kabel di Pusat Data dan/atau area kerja layanan informasi.

Pemeliharaan perangkat-perangkat pengolah informasi dilakukan dengan cara:

a. mencatat daftar perangkat yang digunakan untuk menjalankan informasi;
b. setiap perangkat yang digunakan untuk mengolah informasi dipelihara sesuai dengan buku petunjuk/manualnya;
c. Dalam hal pemeliharaan perangkat pengolah informasi tidak dapat dilakukan di tempat, maka pemindahan perangkat pengolah informasi dilakukan berdasarkan berdasarkan persetujuan Kepala Pusat Data dan Informasi Pembangunan Desa, Daerah Tertinggal, dan Transmigrasi;
d. Dalam hal pemindahan perangkat pengolah informasi terdapat data dan/atau informasi berklasifikasi sangat rahasia dan rahasia yang tersimpan pada perangkat tersebut, maka data dan/atau informasi berklasifikasi sangat rahasia dan rahasia tersebut harus dipindahkan terlebih dahulu ke dalam media penyimpanan lain;
e. Dalam hal pemeliharaan dilakukan oleh Pihak Ketiga, maka pelaksanaannya dilakukan dengan membuat perjanjian Kerjasama;
f. Perjanjian kerjasama paling sedikit memuat perjanjian menjaga kerahasiaan, pemeliharaan yang disediakan, dan tingkat kinerja yang harus dipenuhi Pihak Ketiga.

Pengamanan area dilakukan dengan cara:

a. menyimpan perangkat pengolah informasi di ruangan khusus yang dilindungi dengan pengamanan fisik yang memadai antara lain namun tidak terbatas pada:
   - Pintu dengan kontrol akses
   - Kamera pengawas (CCTV)
   - *Smoke detector*
   - Sistem pemadam kebakaran
   - Perangkat pemutus aliran listrik;
b. akses ke Pusat Data dan/atau area kerja layanan informasi yang berisi data dan/atau informasi rahasia dan rahasia harus dibatasi dan hanya diberikan kepada pegawai yang memiliki akses;
c. Pihak Ketiga yang memasuki Pusat Data dan/atau area kerja layanan informasi yang berisikan data dan/atau informasi rahasia dan rahasia harus didampingi oleh pegawai yang ditugaskan sepanjang waktu kunjungan;
d. makanan dan minuman dilarang untuk dibawa masuk ke atau dikonsumsi di dalam ruang server Pusat Data;
e. semua area yang digunakan untuk menyimpan aset data dan informasi penting merupakan area bebas rokok;
f. batas minimum dan maksimum suhu dan kelembaban di dalam ruang server Pusat Data harus ditetapkan mengikuti standar yang disyaratkan pabrikan perangkat dan senantiasa dilakukan pengawasan terhadap kondisi suhu dan kelembaban;
g. pengamanan area Pusat Data dan area kerja layanan informasi dilakukan sesuai **Prosedur Keamanan Area**;
h. pengamanan kantor, ruangan, dan fasilitas kerja sesuai dengan peraturan dan standar keamanan dan keselamatan kerja;

Perlindungan terhadap ancaman eksternal dan lingkungan dilakukan dengan cara:

a. perangkat pemulihan dan media penyimpanan data cadangan wajib diletakkan di tempat yang aman dengan struktur yang memadai untuk menghindari kerusakan dari bencana (misal: banjir dan gempa);
b. semua perangkat pengolah informasi harus mendapatkan pasokan daya yang sesuai dengan spesifikasi yang diisyaratkan oleh pabrikan perangkat;

c. pasokan listrik yang digunakan untuk mengoperasikan perangkat pengolah informasi harus mempunyai sumber alternatif dengan daya dan jangka waktu ketersediaan atau jangka waktu pengoperasian yang cukup, yang paling sedikit mencakup generator listrik dan *Uniterruptable Power Supply* (UPS) dengan daya yang cukup dan dengan konfigurasi yang dapat memindahkan pasokan listrik tanpa gangguan terhadap perangkat pengolah informasi;
d. bahan berbahaya atau mudah terbakar di lingkungan Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi wajib disimpan pada jarak yang aman dari pusat data dan area kerja layanan informasi; dan
e. perangkat pemadam kebakaran wajib disediakan dan diletakkan di tempat yang mudah dijangkau.

Penempatan dan perlindungan perangkat pengolah informasi dilakukan dengan cara:
a. perangkat diletakkan pada lokasi yang meminimalisir akses pihak yang tidak berwenang;
b. perangkat pengolah informasi yang menangani informasi sensitif diposisikan dan dibatasi sudut pandangnya untuk mengurangi risiko informasi dilihat oleh pihak tidak berwenang;
c. perangkat pengolah informasi yang memerlukan perlindungan khusus wajib terisolasi;
d. kondisi lingkungan, seperti suhu dan kelembaban wajib dimonitor sesuai dengan kebutuhan;
e. perangkat pengolah informasi dilindungi dari kegagalan catu daya dan gangguan lain yang disebabkan kegagalan utilitas pendukung; dan
f. perlindungan petir wajib diterapkan untuk semua bangunan dan filter perlindungan petir dipasang untuk semua jalur komunikasi dan listrik.

Pengamanan kabel di Pusat Data dan/atau area kerja layanan informasi dilakukan dengan mengikuti standar elektrikal/mekanikal Pusat Data yang berlaku.

H. KEAMANAN OPERASIONAL

Keamanan operasional dilakukan untuk memastikan operasional yang aman dan benar pada aset informasi, mengimplementasikan dan memelihara keamanan aset informasi, mengelola layanan yang diberikan oleh Pihak Ketiga, meminimalkan risiko kegagalan, dan melindungi keutuhan dan ketersediaan aset informasi. Keamanan operasional di lingkungan Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi dilakukan oleh Pusat Data dan Informasi Pembangunan Desa, Daerah Tertinggal, dan Transmigrasi dengan cara melakukan pengendalian terhadap hal-hal sebagai berikut:

1. penggunaan perangkat;
2. perencanaan dan penerimaan sistem;
3. program yang membahayakan (*malware*);
4. data cadangan (*back up*); dan
5. Pencatatan *(logging*).

Pengendalian penggunaan perangkat, dilakukan dengan cara:

a. mendokumentasikan, memelihara, dan menyediakan Prosedur Penggunaan Perangkat Pengolah Informasi sesuai dengan peruntukannya;
b. melakukan pemisahan akses terhadap informasi yang memiliki klasifikasi sangat rahasia dan rahasia (seorang pegawai dihindari memiliki akses terhadap seluruh aset informasi dan perangkat pengolahnya); dan
c. memisahkan perangkat pengembangan, pengujian, dan operasional untuk mengurangi risiko perubahan atau akses oleh pihak yang tidak berhak terhadap sistem operasional.

Pengendalian perencanaan dan penerimaan sistem dilakukan dengan cara:

a. memantau penggunaan perangkat pengolah informasi dan membuat perkiraan pertumbuhan kebutuhan ke depan untuk memastikan ketersediaan kapasitas; dan
b. menetapkan kriteria penerimaan untuk sistem informasi baru, pemutakhiran dan versi baru serta melakukan pengujian sebelum penerimaan.

Pengendalian malware dilakukan dengan cara:

a. menerapkan sistem pendeteksian, pencegahan, dan pemulihan, sebagai bentuk perlindungan terhadap ancaman *malware*.
b. Perlindungan dilakukan dengan cara pemasangan paling sedikit meliputi:
   - perangkat *firewall*;
   - perangkat *Intrusion Prevention System* (IPS);
   - perangkat *antivirus*;
   - perangkat manajemen akses pengguna; dan
   - perangkat monitoring / pendukung lainnya sesuai perkembangan teknologi keamanan informasi.
c. melakukan penilaian kerentanan terhadap perangkat pengolah informasi (*vulnerability assessment*) secara berkala dan melakukan tindakan perlindungan terhadap kerentanan dan/atau ancaman yang teridentifikasi.

Pengendalian *backup* dilakukan dengan cara:

a. melakukan pembuatan *backup* informasi dan perangkat lunak yang berada di Pusat Data dan/atau area kerja layanan informasi secara berkala;
b. salinan cadangan data/informasi, perangkat lunak, dan image sistem harus diambil dan diuji secara berkala; dan
c. memproses pembuatan data cadangan sesuai dengan **Prosedur Backup Pusat Data**.

Pengendalian *logging* dilakukan dengan cara:

a. mencatat setiap aktivitas administrator, aktivitas pengguna, peristiwa kegagalan, dan kejadian keamanan dan disimpan dalam periode tertentu;
b. melindungi sistem pencatatan (log) dari pemalsuan dan akses yang tidak berwenang;
c. salinan cadangan data/informasi, perangkat lunak, dan image sistem harus diambil dan diuji secara berkala; dan
d. memproses pembuatan data cadangan sesuai dengan **Prosedur Backup Pusat Data.**

I. Keamanan Komunikasi

Keamanan komunikasi dilakukan untuk memastikan keamanan pertukaran informasi melalui jaringan komunikasi. Keamanan komunikasi di lingkungan Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi dilakukan oleh Pusat Data dan Informasi Pembangunan Daerah Tertinggal, dan Transmigrasi dengan cara melakukan pengendalian terhadap hal-hal sebagai berikut:

1. keamanan jaringan;
2. pertukaran informasi; dan
3. sistem pengolah informasi.

Pengendalian keamanan jaringan dilakukan dengan cara:

a. Pusat Data dan Informasi Pembangunan Daerah Tertinggal, dan Transmigrasi mengidentifikasi fitur keamanan layanan, tingkat layanan, dan kebutuhan pengelolaan dalam kesepakatan penyediaan layanan jaringan termasuk layanan jaringan yang disediakan oleh Pihak Ketiga;
b. dalam hal Pihak Ketiga diizinkan mengakses ke jaringan, maka dilakukan pemantauan serta pencatatan kegiatan selama menggunakan jaringan; dan
c. melindungi jaringan dari pihak yang tidak berhak mengakses, dengan cara:
    - mendokumentasikan arsitektur jaringan yang meliputi seluruh komponen perangkat keras dan perangkat lunak jaringan;
    - menerapkan teknologi keamanan jaringan berbasis enkripsi dan otentikasi (termasuk sertifikat elektronik);
    - menerapkan pemisahan jaringan untuk kelompok pengguna, layanan informasi, dan sistem informasi (informasi dimasukkan ke dalam jaringan sistem informasi).
    - menerapkan parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan; dan
    - menerapkan Prosedur Penggunaan Layanan Jaringan yang membatasi akses ke layanan jaringan atau aplikasi.

Pengendalian pertukaran informasi dilakukan dengan cara:

a. informasi yang terdapat dalam layanan aplikasi informasi yang melewati jaringan publik harus dilindungi dari upaya pengungkapan, modifikasi, dan perusakan dengan menerapkan mekanisme kriptografi;
b. melakukan pendeteksian dan perlindungan terhadap kode berbahaya (malicious code) yang disisipkan pada file yang dikirim melalui sistem elektronik;
c. memberikan perlindungan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan untuk informasi elektronik berklasifikasi sangat rahasia dan rahasia;
d. menetapkan Prosedur Pertukaran Informasi yang mengatur sistem dan keamanan yang digunakan untuk pertukaran informasi.

Pengendalian sistem pengolah informasi dilakukan dengan cara:

a. menerapkan audit *logging* yang mencatat aktivitas pengguna dan kejadian keamanan informasi dalam kurun waktu tertentu untuk membantu investigasi di masa mendatang, antara lain:
    - kegagalan akses;
    - penggunaan hak akses tidak wajar;
    - alokasi dan penggunaan hak akses khusus;
    - penelusuran transaksi pengiriman file sistem atau dokumen tertentu yang mencurigakan; dan
    - penggunaan sumber daya sensitif.
b. menerapkan sistem pencatatan aktivitas administrator dan operator sistem;
c. menerapkan pencatatan kesalahan untuk dianalisis dan diambil tindak pengamanan yang tepat; dan
d. memastikan semua perangkat pengolah informasi yang tersambung dengan jaringan telah disinkronisasi dengan sumber waktu yang akurat dan disepakati.

J. Keamanan Pengembangan dan Pemeliharaan

Keamanan pengembangan dan pemeliharaan sistem dilakukan untuk memastikan bahwa keamanan informasi merupakan bagian yang terintegrasi dalam daur hidup informasi untuk mencegah terjadinya

kesalahan, eksploitasi, modifikasi, dan perusakan sistem informasi oleh pihak yang tidak berwenang. Keamanan pengembangan dan pemeliharaan di lingkungan Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi dilakukan oleh Pusat Data dan Informasi Pembangunan Desa, Daerah Tertinggal, dan Transmigrasi yang mencakup pengendalian terhadap hal-hal sebagai berikut:

1. melakukan pemisahan perangkat pengembangan dan operasional informasi;
2. menerapkan standar keamanan yang relevan dalam proses pembangunan dan pengembangan informasi;
3. melakukan uji kelaikan perangkat pengembangan dan operasional informasi;

Pengendalian pemisahan perangkat pengembangan dan operasional informasi dilakukan dengan cara:

a. lingkungan pengembangan dan operasional aplikasi perangkat pengembangan dan operasional informasi harus dipisahkan baik secara fisik, logic, maupun aksesnya;
b. menjaga agar perangkat pengembangan tidak boleh diakses dari sistem operasional layanan;
c. mengupayakan lingkungan sistem pengujian sama dengan lingkungan sistem operasional layanan;
d. menjaga agar data yang memiliki klasifikasi sangat rahasia dan rahasia tidak boleh disalin ke dalam lingkungan sistem pengujian.

Pengendalian penerapan standar keamanan yang relevan dalam proses pembangunan dan pengembangan infomasi dilakukan dengan cara:

a. memastikan bahwa dalam proses perencanaan dan pembangunan/pengembangan aplikasi dan infrastruktur perangkat informasi termasuk yang dilakukan oleh Pihak Ketiga, telah memasukkan fitur-fitur keamanan dalam spesifikasi aplikasi dan infrastruktur perangkat informasi yang dibangun/dikembangkan;
b. fitur-fitur keamanan yang dimasukkan sesuai dengan standar keamanan relevan, yang mencakup:
    - Standar keamanan data dan informasi;
    - Standar keamanan aplikasi;
    - Standar keamanan pusat data;

- Standar keamanan sistem penghubung layanan; dan
- Standar keamanan jaringan intra.

c. standar keamanan sebagaimana dimaksud pada butir b mengacu pada standar keamanan yang ditetapkan oleh Lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber.

Pengendalian uji kelaikan perangkat pengembangan dan operasional informasi dilakukan dengan cara:

a. melaksanakan uji kelaikan perangkat pengembangan dan operasional informasi sebelum perangkat informasi digunakan dan sewaktu-waku sesuai kebutuhan, yang mencakup aspek:
   - uji fungsi, yaitu pengujian yang memastikan perangkat informasi yang dibangun dan/atau dikembangkan telah memenuhi fungsi-fungsi sesuai dengan dokumentasi terkait;
   - uji integrasi, yaitu pengujian yang memastikan perangkat informasi yang dibangun dan/atau dikembangkan telah memenuhi kebutuhan dan persyaratan integrasi dengan aplikasi, data, serta komponen-komponen lain yang terkait;
   - uji beban, yaitu pengujian yang yang memastikan perangkat informasi yang dibangun dan/atau dikembangkan dapat berfungsi sebagaimana mestinya menghadapi beban kerja yang dikenakan terhadapnya;
   - uji keamanan, yaitu pengujian yang memastikan perangkat informasi yang dibangun dan/atau dikembangkan dapat menjaga keamanan data dan informasi yang terkait dengannya.
b. 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 informatika;
c. uji keamanan dapat menggunakan pedoman / instrumen pengukuran yang ditetapkan oleh Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber; dan
d. jika sistem operasi yang digunakan diubah, maka aplikasi informasi yang berjalan di atasnya harus dievaluasi dan diuji kembali untuk menjamin keutuhan sistem tidak terganggu;

Pelaksanaan pembangunan dan pengembangan aplikasi informasi dilakukan sesuai dengan Standar Teknis dan Prosedur Pembangunan dan Pengembangan Aplikasi SPBE yang ditetapkan oleh Kementerian yang melaksanakan tugas di bidang Komunikasi dan Informatika.

K. Keamanan Pihak Ketiga

Keamanan Pihak Ketiga dilakukan untuk memastikan perlindungan dari aset informasi yang dapat diakses oleh Pihak Ketiga. Keamanan Pihak Ketiga di lingkungan Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi dilakukan oleh Pusat Data dan Informasi Pembangunan Desa, Daerah Tertinggal, dan Transmigrasi dengan cara melakukan pengendalian terhadap hal-hal sebagai berikut:

1. melakukan pemeriksaan latar belakang Pihak Ketiga dengan tetap memperhatikan privasi dan perlindungan data pribadi;
2. membuat perjanjian tertulis dengan pihak ketiga yang terlibat dalam penggunaan dan/atau pengelolaan informasi yang menyatakan tanggung jawab terhadap keamanan informasi. Perjanjian tertulis sebagaimana dimaksud paling sedikit memuat:
   a. perlindungan atas informasi rahasia dan hak kekayaan intelektual setiap pihak;
   b. dalam hal aset informasi disediakan oleh Pihak Ketiga, maka adanya jaminan bahwa tidak terdapat malicious code dan backdoor;
   c. hak untuk melakukan audit dan memantau kegiatan yang melibatkan informasi rahasia;
   d. pelaporan terhadap penyingkapan yang dilakukan secara tidak sah atau pelanggaran terhadap kerahasiaan; dan
   e. syarat untuk informasi yang akan dikembalikan atau dimusnahkan pada saat penghentian perjanjian.
   f. dalam hal Pihak Ketiga tidak lagi menjadi bagian dalam pengelolaan aset informasi, maka aset informasi yang dikuasainya diserahkan kembali Pusat Data dan Informasi Pembangunan Desa, Daerah Tertinggal, dan Transmigrasi.
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. pengaturan SLA terkait 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 resiko 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;
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 lingkungan Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi;
10. membuat berita acara serah terima terkait mengembalikan seluruh aset informasi yang dipergunakan selama bekerja bagi Pihak Ketiga yang berakhir masa kontraknya; dan

memastikan pihak Ketiga dan tamu yang memasuki lingkungan area Pusat Data, dan tempat layanan informasi harus mematuhi standar keamanan fisik dan lingkungan.

L. Manajemen Insiden Keamanan Siber

Manajemen insiden keamanan siber dilaksanakan untuk mengendalikan gangguan keamanan informasi. Insiden keamanan siber termasuk namun tidak terbatas pada:

- *Web defacement*;
- *Malware (virus, worm, trojan backdoor*);
- *Ransomware;*
- *Unauthorized access;*
- *Data breach;*
- *Distributed Denial of Service.*

Manajemen insiden keamanan siber di lingkungan Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi dilakukan oleh Pusat Data dan Informasi Pembangunan Desa, Daerah Tertinggal, dan Transmigrasi dengan cara sebagai berikut:

1. membentuk *Computer Security Incident Response Team* (CSIRT / Tim Respon Insiden) yang bertugas melakukan pencegahan dan penanganan insiden keamanan siber yang terjadi di lingkungan Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi;
2. Tim Respon Insiden melakukan tindakan pencegahan insiden keamanan siber yang meliputi:
   a. melakukan penilaian kerentanan dan/atau penetration testing untuk menemukan kelemahan keamanan informasi dalam sistem layanan informasi;
   b. mengimplementasikan alat monitoring keamanan berupa SIEM; dan
   c. melakukan monitoring dan pendeteksian serangan terhadap sistem layanan informasi.
3. Dalam hal terjadi insiden keamanan siber, Tim Respon Insiden melaksanakan Prosedur Penanganan Insiden Keamanan Siber yang meliputi:
   a. menerima laporan dan mencatat insiden keamanan siber;
   b. mengidentifikasi sumber serangan;
   c. menganalisis informasi yang berkaitan dengan insiden keamanan siber;
   d. memprioritaskan penanganan insiden berdasarkan tingkat dampak;
   e. mendokumentasikan bukti insiden keamanan siber;
   f. menyusun laporan penanganan insiden keamanan siber; dan
   g. mengevaluasi dan memperbaiki standar, prosedur, dan kontrol-kontrol keamanan informasi agar insiden keamanan siber serupa tidak terulang kembali di masa mendatang.
4. menyusun berbagai macam skenario penanganan insiden keamanan siber;
5. melakukan simulasi skenario penanganan insiden keamanan siber yang telah disusun secara berkala;
6. memberikan pelatihan terhadap SDM internal yang terlibat pada penanganan insiden sesuai skenario yang disusun;
7. menjalankan program kesadaran ancaman dan penanganan insiden, serta ajakan peran aktif pada seluruh karyawan; dan

melakukan pengukuran tingkat kematangan penanganan insiden secara berkala.

M. 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 Pusat Data dan Informasi Pembangunan Desa, Daerah Tertinggal, dan Transmigrasi dengan cara sebagai berikut:

1. melakukan identifikasi risiko terhadap keberlangsungan layanan informasi;
2. menyusun dan menerapkan rencana keberlangsungan layanan informasi (*Business Continuity Planning*) untuk menjaga dan mengembalikan operasional informasi dalam jangka waktu yang disepakati dan tingkat keberlangsungan yang dibutuhkan;
3. rencana keberlangsungan layanan informasi paling sedikit meliputi:
    a. Prosedur Keberlangsungan Layanan Informasi pada saat keadaan darurat, manajemen risiko, analisis dampak kegiatan, pengembalian kondisi semula (*fallback*), peralihan kondisi normal, dan ujicoba keberlangsungan kegiatan;
    b. penetapan peran dan penanggungjawab pegawai yang terlibat dalam pelaksanaan keberlangsungan layanan informasi;
    c. pelaksanaan sosialisasi dan pelatihan keberlangsungan layanan informasi;
4. jika aplikasi informasi merupakan aplikasi umum / SE 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. melaksanakan proses keberlangsungan layanan infomasi pada saat keadaan darurat sesuai prosedur keberlangsungan layanan informasi;

N. Pengendalian Kepatuhan

Pengendalian kepatuhan dilaksanakan untuk memastikan kepatuhan pegawai dan Pihak Ketiga dalam melaksanakan Keamanan informasi

sesuai dengan ketentuan peraturan perundang-undangan. Pengendalian kepatuhan keamanan informasi di lingkungan Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi, dilakukan oleh Pelaksana Teknis Keamanan Informasi dengan cara sebagai berikut:

1. mengidentifikasi, mendokumentasikan, dan memelihara regulasi terkait keamanan informasi;
2. memeriksa kepatuhan seluruh pegawai dan Pihak Ketiga terhadap regulasi, standar, dan prosedur keamanan informasi;
3. mendapatkan perangkat lunak hanya melalui sumber yang dikenal dan memiliki reputasi baik, untuk memastikan tidak ada pelanggaran hak cipta;
4. memeriksa kepatuhan penggunaan lisensi perangkat lunak dan menerapkan pengendalian untuk memastikan jumlah pengguna tidak melampaui lisensi yang dimiliki;
5. memelihara bukti kepemilikan lisensi, master disk, buku manual, dan lain sebagainya;
6. melakukan pemeriksaan bahwa tidak ada produk bajakan yang terinstall (pelanggaran hak kekayaan intelektual);

O. 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 dan Audit Eksternal yang dilaksanakan dengan cara sebagai berikut:

1. Audit Internal Keamanan Informasi
   a. Audit Internal Keamanan Informasi di lingkungan Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi dilaksanakan oleh Inspektorat Jenderal dan dapat bekerjasama dengan Pelaksana Teknis Keamanan Informasi;
   b. Inspektorat Jenderal merencanakan, menetapkan, dan menjalankan program audit mencakup frekuensi, metode, kriteria, tanggung jawab, dan pelaporan audit;
   c. Audit Internal Keamanan Informasi dilaksanakan minimal satu kali dalam satu tahun dan dimasukkan dalam Peta Rencana SPBE

Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi;

d. Audit Internal Keamanan Informasi dilaksanakan oleh Auditor yang memiliki kompetensi memadai dan memiliki objektifitas serta imparsialitas (ketidakberpihakan) dalam melaksanakan Audit Internal Keamanan Informasi.
e. Setiap temuan audit harus dicatat secara formal oleh Auditor dan diberikan kepada auditee.
f. Auditee harus melakukan perbaikan terhadap setiap temuan yang diberikan oleh Auditor dalam jangka waktu yang disepakati.
g. Laporan Audit Internal dilaporkan kepada Pelaksana Teknis Keamanan Informasi sebagai bahan evaluasi penerapan kebijakan keamanan informasi.
h. 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;
i. Audit Internal Keamanan Informasi dilaksanakan sesuai dengan Prosedur Audit Internal Keamanan Informasi;

2. Audit Eksternal Keamanan Informasi
   a. Audit Eksternal Keamanan Informasi di lingkungan Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi dilaksanakan oleh Pihak Ketiga yang berkompeten;
   b. Dalam hal aplikasi informasi merupakan Aplikasi Umum dan/atau Sistem Elektronik berkategori Strategis maka Audit Eksternal Keamanan Informasi dilaksanakan paling sedikit satu kali dalam satu tahun oleh Lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber dan sandi;
   c. Dalam hal aplikasi informasi merupakan Aplikasi Khusus maka Audit Eksternal Keamanan Informasi dilaksanakan paling sedikit satu kali dalam dua tahun oleh Lembaga Audit TIK yang teregistrasi pada Lembaga yang menjalankan tugas pemerintahan di bidang keamanan siber dan sandi;
   d. Pelaksanaan audit eksternal keamanan informasi menggunakan instrumen penilaian Audit Keamanan SPBE yang ditetapkan oleh

Kepala Lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber;

e. Audit Eksternal keamanan informasi dilaksanakan sesuai dengan peraturan mengenai Standar dan Tata Cara Pelaksanaan Audit Keamanan SPBE yang berlaku.

P. Evaluasi Kinerja Keamanan Informasi

Evaluasi kinerja keamanan informasi dilaksanakan paling sedikit satu kali dalam satu tahun untuk memastikan pencapaian target keamanan informasi yang telah direncanakan. Kepala Badan Pengembangan dan Informasi Desa, Daerah Tertinggal, dan Transmigrasi dengan dibantu Pelaksana Teknis Keamanan Informasi melakukan evaluasi kinerja pelaksanaan keamanan informasi berdasarkan peta rencana yang telah ditetapkan, dengan cara sebagai berikut:

1. mengidentifikasi kegiatan-kegiatan yang memiliki risiko tinggi terhadap keberhasilannya;
2. menetapkan indikator kinerja pada setiap kegiatan dan menetapkan secara kuantitatif kinerja yang diharapkan;
3. mengukur capaian kinerja dan efektifitas penerapan keamanan SPBE;
4. mendukung dan merealisasikan kegiatan audit keamanan SPBE sebagai bagian dari evaluasi penerapan keamanan SPBE; dan
5. melakukan langkah-langkah perbaikan untuk mencapai target indikator kinerja dan memperbaiki hasil temuan audit.

BAB III

PENUTUP

Keputusan Menteri Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi tentang Kebijakan dan Standar Sistem Manajemen Keamanan Informasi Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi ini ditetapkan sebagai pedoman dalam melindungi aset informasi Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi dari berbagai bentuk ancaman baik dari dalam maupun dari luar, dengan tujuan untuk menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi.

Hal-hal yang sifatnya terlalu teknis dan spesifik yang belum diatur dalam Keputusan Menteri Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi ini, secara khusus akan diatur dalam buku pedoman, atau dapat dilaksanakan langsung sesuai dengan standar operasional prosedur.

MENTERI DESA,
PEMBANGUNAN DAERAH TERTINGGAL, DAN TRANSMIGRASI
REPUBLIK INDONESIA,

ttd.

ABDUL HALIM ISKANDAR

Salinan sesuai aslinya
Kementerian Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi
Plt. Kepala Biro Hukum

Rully Rachman