



**ARSIP NASIONAL
REPUBLIK INDONESIA**

**KEPUTUSAN KEPALA ARSIP NASIONAL REPUBLIK INDONESIA
NOMOR 273 TAHUN 2026
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI
DI LINGKUNGAN ARSIP NASIONAL REPUBLIK INDONESIA**

KEPALA ARSIP NASIONAL REPUBLIK INDONESIA,

- Menimbang :
- a. bahwa untuk melindungi keamanan informasi berdasarkan hasil pengukuran tingkat kematangan keamanan siber dan persandian menggunakan Instrumen Pengukuran Tingkat Kematangan Keamanan Siber dan Sandi (IKASANDI) dan rencana tindak lanjut hasil Audit Keamanan Aplikasi Umum Bidang Kearsipan Dinamis Sistem Informasi Kearsipan Dinamis Terintegrasi (SRIKANDI), diperlukan Sistem Manajemen Keamanan Informasi di lingkungan Arsip Nasional Republik Indonesia;
 - b. bahwa Keputusan Kepala Arsip Nasional Republik Indonesia Nomor 223 Tahun 2025 tentang Sistem Manajemen Keamanan Informasi di Lingkungan Arsip Nasional Republik Indonesia dipandang sudah tidak sesuai lagi dengan perkembangan hukum dan kebutuhan organisasi sehingga perlu diganti;
 - c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Keputusan Kepala Arsip Nasional Republik Indonesia tentang Sistem Manajemen Keamanan Informasi di Lingkungan Arsip Nasional Republik Indonesia;

- Mengingat : 1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843), sebagaimana telah beberapa kali diubah terakhir dengan 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);
2. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
3. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038);
4. Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi, (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820);
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 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

7. Peraturan Presiden Nomor 23 Tahun 2023 tentang Arsip Nasional Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 52);
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);
9. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2024 tentang Standar dan Tata Cara Pelaksanaan Audit Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2024 Nomor 655);
10. Peraturan Arsip Nasional Republik Indonesia Nomor 2 Tahun 2024 tentang Organisasi dan Tata Kerja Arsip Nasional Republik Indonesia (Berita Negara Republik Indonesia Tahun 2024 Nomor 89);

MEMUTUSKAN:

Menetapkan : KEPUTUSAN KEPALA ARSIP NASIONAL REPUBLIK INDONESIA TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN ARSIP NASIONAL REPUBLIK INDONESIA.

KESATU : Menetapkan Sistem Manajemen Keamanan Informasi di Lingkungan Arsip Nasional Republik Indonesia, sebagaimana tercantum dalam lampiran yang merupakan bagian tidak terpisahkan dari Keputusan ini.

KEDUA : Sistem Manajemen Keamanan Informasi sebagaimana dimaksud dalam DIKTUM KESATU dilaksanakan oleh

seluruh unit kerja di lingkungan Arsip Nasional Republik Indonesia dan pihak ketiga yang merupakan pengelola dan/atau pengguna teknologi informasi dan komunikasi dengan mendefinisikan ruang lingkup dan batas-batas manajemen keamanan informasi SPBE yang mempertimbangkan kebutuhan pemangku kepentingan, isu internal dan eksternal.

KETIGA : Pada saat Keputusan Kepala ini mulai berlaku, Keputusan Kepala Arsip Nasional Republik Indonesia Nomor 223 Tahun 2025 tentang Sistem Manajemen Keamanan Informasi di Lingkungan Arsip Nasional Republik Indonesia dicabut dan dinyatakan tidak berlaku.

KEEMPAT : Keputusan Kepala ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta

pada tanggal 8 September 2026

KEPALA ARSIP NASIONAL REPUBLIK INDONESIA,



MEGO PINANDITO

LAMPIRAN

KEPUTUSAN KEPALA ARSIP NASIONAL REPUBLIK INDONESIA
NOMOR 273 TAHUN 2026
TANGGAL 8 SEPTEMBER 2026

SISTEM MANAJEMEN KEAMANAN INFORMASI
DI LINGKUNGAN ARSIP NASIONAL REPUBLIK INDONESIA

BAB I
PENDAHULUAN

1. Latar Belakang

Keamanan Informasi merupakan hal penting dalam penyelenggaraan layanan. Dalam rangka menunjang pelaksanaan Sistem Pemerintahan Berbasis Elektronik, diperlukan suatu Sistem Manajemen Keamanan Informasi untuk menunjang keandalan dan keamanan sistem elektronik. Keamanan informasi didasarkan kepada 5 (lima) aspek, yaitu:

- a. Aspek kerahasiaan yaitu jaminan bahwa informasi yang menjadi kewenangan Arsip Nasional Republik Indonesia dijamin tidak dapat diketahui/diakses oleh pihak yang tidak berwenang;
- b. Aspek keaslian yaitu adanya jaminan kepastian terhadap informasi yang ditransaksikan dalam sistem informasi bersumber dari pihak yang sah;
- c. Aspek keutuhan yaitu adanya jaminan bahwa informasi yang menjadi kewenangan Arsip Nasional Republik Indonesia dijamin tidak dapat diubah tanpa izin pihak yang berwenang, informasi selalu lengkap dan konsisten, serta terjaga dari kerusakan atau ancaman lain yang dapat menyebabkan perubahan atas informasi awal/asli;
- d. Aspek kenirsangkalan yaitu adanya jaminan bahwa tidak dapat disangkalnya oleh seseorang atau pihak tertentu atas tindakan yang telah dilakukan dalam penggunaan suatu sistem informasi; dan
- e. Aspek ketersediaan yaitu adanya jaminan bahwa informasi selalu tersedia untuk berbagai keperluan yang sesuai dengan

ketentuan peraturan perundang-undangan, baik untuk pengaksesan maupun untuk keperluan transaksi.

Sehubungan dengan hal tersebut, dalam rangka keamanan informasi di lingkungan Arsip Nasional Republik Indonesia, perlu menyusun sebuah standar tentang Sistem Manajemen Keamanan Informasi yang mengatur bagaimana informasi menjadi aman agar kerahasiaan, keaslian, keutuhan, kenirsangkalan, dan ketersediaan informasi tetap terjaga.

2. Maksud dan Tujuan

Sistem Manajemen Keamanan Informasi ini digunakan sebagai pedoman atau standar untuk melindungi informasi elektronik dari berbagai bentuk ancaman baik dari dalam maupun luar lingkungan Arsip Nasional Republik Indonesia, dengan tujuan untuk menjamin kerahasiaan, keaslian, keutuhan, kenirsangkalan, dan ketersediaan informasi.

3. Ruang Lingkup

Ruang Lingkup Sistem Manajemen Keamanan Informasi mencakup:

- a. proses sistem manajemen keamanan informasi;
- b. penetapan penanggung jawab;
- c. perencanaan;
- d. dukungan pengoperasian;
- e. evaluasi kinerja; dan
- f. perbaikan berkelanjutan.

4. Pengertian

- a. Sistem Manajemen Keamanan Informasi adalah bagian dari keseluruhan sistem manajemen untuk menetapkan, menerapkan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan keamanan informasi yang dibangun dengan pendekatan risiko untuk mencapai visi dan misi lembaga.
- b. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *Electronic Data Interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

- c. Arsip Nasional Republik Indonesia, yang selanjutnya disebut ANRI adalah lembaga kearsipan berbentuk lembaga pemerintah non kementerian yang melaksanakan tugas negara di bidang kearsipan yang berkedudukan di ibu kota negara.
- d. Infrastruktur Teknologi Informasi dan Komunikasi adalah seluruh perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat elektronik lainnya.
- e. Aplikasi adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi layanan di bidang teknologi informasi.
- f. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
- g. Pejabat Sistem Keamanan Informasi adalah Pejabat Pimpinan Tinggi Pratama yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi di lingkungan ANRI.
- h. Pejabat Pengelola Informasi adalah seluruh Pejabat Pimpinan Tinggi Pratama di lingkungan ANRI.
- i. Komite Keamanan Informasi adalah koordinator dan pengarah atas terlaksananya penerapan kebijakan dan efektivitas pelaksanaan keamanan informasi di lingkungan ANRI.
- j. Sistem Operasi adalah perangkat lunak sistem yang mampu mengelola sumber daya (*resources*) dari *software* dan *hardware* agar dapat berjalan dengan baik serta memudahkan proses interaksi dengan pengguna.
- k. Jaringan adalah hubungan dua atau lebih perangkat yang saling terhubung atau terkoneksi antara satu dengan yang lain dan digunakan untuk berbagi sumber data.
- l. Kode Sumber adalah suatu rangkaian perintah, pernyataan, dan/atau deklarasi yang ditulis dalam bahasa pemrograman komputer yang dapat dibaca dan dipahami.

- m. Hak Akses adalah izin yang diberikan untuk memperoleh aset informasi.
- n. Kriptografi adalah disiplin ilmu yang meliputi prinsip, sarana dan metode untuk menyediakan keamanan informasi, termasuk kerahasiaan, integritas data, autentikasi dan nir-penyangkalan.
- o. Pihak Ketiga adalah seluruh unsur di luar pengguna ANRI, seperti mitra kerja, konsultan, penyedia jasa komunikasi, pemasok, dan pemelihara perangkat pengolah informasi, dan ANRI/lembaga lain.

BAB II

PROSES SISTEM MANAJEMEN

KEAMANAN INFORMASI

Sistem Manajemen Keamanan Informasi dilaksanakan oleh seluruh unit kerja ANRI dan Pihak Ketiga yang merupakan pengelola dan/atau pengguna teknologi informasi dan komunikasi. Dalam rangka melaksanakan Sistem Manajemen Keamanan Informasi tersebut perlu dibuat suatu pedoman yang mengatur mengenai Sistem Manajemen Keamanan Informasi dengan ruang lingkup:

A. Informasi

Informasi mencakup informasi tercetak, tertulis dan tersimpan dalam bentuk elektronik seperti *database*, pada *file* di dalam komputer, ditampilkan pada *website*, layar komputer dan dikirimkan melalui jaringan telekomunikasi. Pelaksanaan Sistem Manajemen Keamanan Informasi harus memenuhi standar teknis keamanan informasi elektronik. Adapun standar teknis tersebut mencakup:

1. Klasifikasi Informasi

Setiap informasi elektronik diklasifikasikan berdasarkan prasyarat hukum, nilai informasi, tingkat kekritisian dan kepekaan untuk menghindari pengungkapan secara tidak sah (*unauthorised disclosure*). Klasifikasi informasi dibagi dalam 4 klasifikasi dengan pengaturan sebagai berikut:

- a. Sangat Rahasia adalah informasi yang memiliki tingkat risiko sangat tinggi dan berdampak sangat serius bagi kelancaran dan keberhasilan dalam operasional di ANRI diberi tanda khusus (label) "SANGAT RAHASIA".
- b. Rahasia adalah informasi yang memiliki risiko tinggi bagi operasional di ANRI diberi tanda khusus (label) "RAHASIA".
- c. Terbatas adalah informasi yang bersifat rutin yang mempunyai kepekaan, nilai dan risiko sedang, hanya berlaku untuk kepentingan internal ANRI atau bukan termasuk informasi publik, diberi tanda khusus (label) "TERBATAS".
- d. Biasa/Terbuka adalah informasi yang memiliki risiko rendah atau tanpa risiko boleh diketahui oleh semua khalayak baik internal dan eksternal ANRI sesuai dengan ketentuan peraturan perundang-undangan tidak perlu diberi tanda khusus (label).

Klasifikasi informasi juga harus mempertimbangkan kebutuhan layanan ANRI, dampak terhadap layanan ANRI dan pelaksanaan tugas dan fungsi ANRI apabila terjadi kegagalan keamanan informasi elektronik.

2. Pengelolaan Informasi

a. Prinsip Pelaksanaan Pengelolaan Informasi

- 1) Unit kerja pemilik informasi selaku pemilik proses bisnis bertanggung jawab untuk:
 - a) Mengklasifikasikan informasi yang dimilikinya ke dalam klasifikasi informasi yang telah ditetapkan;
 - b) Melakukan pencatatan atas informasi berdasarkan klasifikasi informasi ke dalam suatu dokumen register; dan
 - c) Melakukan peninjauan klasifikasi informasi secara periodik untuk memastikan bahwa klasifikasi telah sesuai dengan kondisi dan kebutuhan ANRI terkini (*up to date*).

2) Penanganan Informasi dan Pemberian Tanda

- a) Prosedur terkait dengan pemberian tanda dan penanganan informasi ditetapkan oleh Pejabat Sistem Keamanan Informasi dan Pejabat Pengelola Informasi dan diimplementasikan berdasarkan sistem klasifikasi informasi ANRI sesuai dengan kebutuhan unit kerja masing-masing.
- b) Penanganan Informasi khususnya yang bersifat rahasia dan sangat rahasia mencakup pada aspek pemrosesan, penyimpanan, distribusi, dan pemusnahan harus diterapkan secara aman.
- c) Prosedur pemberian tanda/pelabelan informasi harus mencakup segala bentuk informasi.
- d) Data/informasi yang tersimpan dalam media elektronik harus mendapatkan perlakuan sesuai kerahasiaannya dan diusahakan diberikan password atau pembatasan akses ke folder.
- e) Pemilik Informasi wajib melakukan pencadangan atas informasi yang dimiliki setiap kali telah menerima dan/atau memproduksi informasi berdasarkan tingkat kerahasiaan atau kritikalitas informasi.
- f) Pencadangan dilakukan melalui media penyimpanan

yang telah ditentukan oleh Pejabat Sistem Keamanan Informasi.

- 3) Prosedur penanganan informasi, yang mencakup proses penyimpanan dan pemindahan harus didefinisikan dengan jelas untuk setiap kategori klasifikasi.
- 4) Perlindungan terhadap informasi yang bersifat rahasia harus disesuaikan dengan tingkat keamanan yang memadai sesuai dengan aturan penanganan informasi yang ditetapkan di ANRI.
- 5) Penetapan prosedur pemberian tanda pada informasi setidak- tidaknya harus sesuai dengan penanganan dan klasifikasi informasi sebagai berikut:

Klasifikasi Tipe	Publik	Terbatas	Rahasia/ Sangat Rahasia
Penyimpanan informasi di dalam <i>personal computer</i> atau laptop	Tidak diperlukan penanganan khusus	<i>Screen saverlock</i> harus aktif jika meninggalkan komputer/ laptop	<i>Screen saverlock</i> harus aktif jika meninggalkan komputer/laptop
Penyimpanan informasi di dalam <i>removable media</i>	Tidak diperlukan penanganan khusus	<i>Removable media</i> harus diberikan <i>password</i>	<i>Removable media</i> harus diberikan <i>password</i>
Penyimpanan informasi dalam <i>share folder</i>	Tidak diperlukan penanganan khusus	Folder harus diberikan <i>password</i>	• Folder harus diberikan <i>password</i> • Informasi harus diberikan <i>password</i>
Penyimpanan informasi di dalam <i>Server</i> ANRI	Akses <i>server</i> menggunakan <i>credential</i> yang terdaftar	Akses <i>server</i> menggunakan <i>credential</i> yang terdaftar	Akses <i>server</i> menggunakan <i>credential</i> yang terdaftar
Penyimpanan pada pihak ketiga	Tidak diperlukan penanganan khusus	Harus disertai dengan perjanjian kerahasiaan (<i>non disclosure agreement</i>)	Harus disertai dengan perjanjian kerahasiaan (<i>non disclosure agreement</i>)

Klasifikasi Tipe	Publik	Terbatas	Rahasia/ Sangat Rahasia
Pengiriman ke pihak internal melalui <i>e-mail</i>	Pengiriman <i>e-mail</i> harus menggunakan <i>account e-mail</i> ANRI	Pengiriman <i>e-mail</i> harus menggunakan <i>account e-mail</i> ANRI	• Pengiriman <i>e-mail</i> harus menggunakan <i>account e-mail</i> ANRI • Melakukan enkripsi pada informasi yang dikirim melalui <i>e-mail</i>
Pengiriman ke pihak eksternal melalui <i>e-mail</i>	Pengiriman <i>e-mail</i> menggunakan <i>account e-mail</i> ANRI	• Pengiriman <i>e-mail</i> menggunakan <i>account e-mail</i> ANRI • Pastikan alamat <i>e-mail</i> tujuan sudah benar	• Pengiriman <i>e-mail</i> menggunakan <i>account e-mail</i> ANRI • Pastikan alamat <i>e-mail</i> tujuan sudah benar • <i>File</i> informasi yang dikirimkan harus dienkripsi atau di <i>password</i>

b. Pengelolaan Pertukaran Informasi

Pengelolaan Pertukaran Informasi meliputi hal-hal sebagai berikut:

1) Kebijakan dan Prosedur Pertukaran Informasi

Pertukaran Informasi dengan menggunakan fasilitas *e-mail* harus memperhatikan perlindungan terhadap informasi yang dipertukarkan (dalam bentuk *attachment*) dari salah pengiriman atau perusakan. Jika dimungkinkan, perlu digunakan *password* untuk melindungi kerahasiaan, integritas dan keaslian informasi elektronik yang dipertukarkan.

Hal-hal berikut perlu dipertimbangkan pada saat proses pertukaran informasi:

- a) Pengamanan pertukaran informasi dilakukan untuk melindungi dari ancaman *interception*, *copying*, modifikasi, *misrouting*, dan perusakan.
- b) Kebijakan *Zero Trust* dan *Multi-Factor Authentication* (MFA). Pengamanan sistem informasi arsip digital harus menerapkan prinsip *Zero Trust* dan penguatan autentikasi melalui mekanisme *Multi-Factor Authentication* (MFA), khususnya untuk sistem yang

mengelola arsip rahasia. Pengendalian akses oleh layanan otomatis (Bot/API), skrip otomatis dan API yang mengakses arsip digital harus didaftarkan dan diaudit secara berkala. Akses bot hanya diberikan berdasarkan peran, fungsi, dan otorisasi yang sah.

- c) MFA diterapkan paling sedikit pada akun berhak istimewa, akses jarak jauh, Sistem Elektronik berkategori strategis atau kritis, serta Sistem Elektronik yang memproses Data Pribadi atau informasi berklasifikasi Terbatas, Rahasia, dan Sangat Rahasia, sesuai hasil penilaian risiko.
- d) Perlindungan informasi dari *malware* yang dapat ditransmisikan melalui penggunaan media komunikasi elektronik.
- e) Pengaturan tata cara penggunaan media komunikasi elektronik seperti *e-mail* dan *internet*.
- f) Penggunaan media komunikasi *wireless* secara aman.
- g) Penetapan kebijakan dan pedoman terkait *acceptable use of electronic communication*.
- h) Sosialisasi *awareness* kepada seluruh pegawai agar bertanggung jawab dalam bertukar informasi sehingga tidak menyebabkan berkurangnya reputasi ANRI, seperti melakukan pencemaran nama baik, *impersonation*, pelecehan atau pengiriman surat kaleng.
- i) Sosialisasi *awareness* agar pegawai berhati-hati apabila berkomunikasi di ruang publik dan ruang siber (*cyber space*).
- j) Penggunaan kriptografi untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi yang dipertukarkan.
- k) Informasi sensitif tidak ditinggalkan pada fasilitas pencetakan seperti mesin fotokopi, *printer*, mesin *fax* tanpa pengawasan.
- l) Penerapan kontrol untuk mengatur atau melarang *automatic forwarding* dalam penggunaan layanan informasi elektronik, seperti *automatic e-mail forwarding* dari *e-mail* ANRI ke *e-mail* pribadi.

- m) Tidak meninggalkan informasi sensitif pada *answering machine*.
- n) Menjaga prinsip kehati-hatian dalam menggunakan mesin *faximile*.
- o) Pembatasan atau larangan untuk memberikan data pribadi yang bersifat umum dan khusus. Data pribadi bersifat umum seperti nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan dan/atau Data Pribadi yang dikombinasikan untuk mendefinisikan seseorang. Data Pribadi bersifat khusus seperti data dan informasi Kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi, dan/atau data lainnya sesuai peraturan perundang-undangan. Data dan Informasi Pribadi tersebut dapat disalahgunakan oleh pihak luar.
- p) Pembatasan atau larangan untuk memberikan data pribadi seperti alamat *e-mail* atau data pribadi lainnya yang mungkin dapat disalahgunakan oleh pihak luar.
- q) *Cache* pada *printer* dan mesin fotokopi harus dipastikan terhapus.
- r) Pegawai tidak diperbolehkan melakukan percakapan mengenai informasi rahasia ANRI di tempat umum dan ruang siber yang terbuka.

2) Perjanjian Pertukaran Data dan Informasi

- a) Dalam melaksanakan pertukaran data dan informasi harus dipastikan adanya perjanjian formal pertukaran informasi dengan pihak lain untuk memastikan semua pihak yang terlibat melakukan pengamanan informasi. Perjanjian tersebut sekurang-kurangnya memuat hal-hal sebagai berikut:
 - (1) Kesepakatan dalam kesepahaman yang sama terkait keamanan informasi sehingga informasi dapat dilindungi secara memadai.
 - (2) Penyimpanan informasi secara aman dan memadai.
 - (3) Penggunaan sistem pelabelan yang telah disepakati untuk informasi yang sensitif serta memastikan bahwa sistem tersebut dapat dengan mudah

dimengerti.

(4) Penggunaan teknologi *password* yang sesuai standar.

b) Kesepakatan atau perjanjian tersebut harus mempertimbangkan aspek-aspek keamanan sebagai berikut:

(1) Tanggung jawab dalam melakukan pengendalian dan notifikasi transmisi informasi, *dispatch*, dan penerimaan informasi.

(2) Standar teknis dalam pengemasan dan transmisi.

(3) Perjanjian *escrow* yang merupakan perjanjian yang mengatur lisensi dan *source code* dari *software* dengan pihak ketiga selaku penyedia *software*.

(4) Tugas dan tanggung jawab pada saat terjadinya insiden keamanan informasi seperti kehilangan data.

(5) Kepemilikan dan tanggung jawab untuk perlindungan data, *copyright* dan kepatuhan pada hukum lisensi.

(6) Penggunaan teknologi kriptografi.

3) Pesan Elektronik (*e-mail*)

a) Pengiriman informasi milik ANRI menggunakan metode pesan elektronik, seperti *e-mail* dan *file sharing* harus dilindungi untuk menghindari kebocoran informasi secara tidak disengaja akibat kesalahan pengiriman atau ketiadaan pengamanan pada file.

b) Pengamanan Metadata dan Jejak Audit Arsip Digital. Metadata arsip digital harus dilindungi dari manipulasi dan pemalsuan. Setiap perubahan pada arsip digital harus tercatat secara otomatis dalam sistem log audit yang tidak dapat dihapus, guna menjamin prinsip akuntabilitas dan kenirsangkalan.

c) Perlindungan tersebut perlu mempertimbangkan aspek- aspek berikut:

(1) *Awareness* kepada pengguna untuk memastikan keamanan dalam penggunaan fasilitas pesan elektronik;

(2) Keamanan informasi yang dikirimkan

menggunakan media pesan elektronik dipastikan sesuai dengan klasifikasinya;

- (3) Digunakan teknologi kriptografi untuk menjaga kerahasiaan dan integritas dari informasi yang dikirimkan serta untuk memastikan identitas tujuan pengiriman;
 - (4) Pembatasan penggunaan layanan pesan elektronik yang bersifat publik untuk mengirimkan informasi.
- d) Setiap Aparatus Sipil Negara (ASN) aktif di ANRI berhak mendapatkan alamat *e-mail* dinas untuk keperluan komunikasi dan kolaborasi guna melaksanakan tugas yang berkaitan dengan ANRI.
 - e) *E-mail* dinas dapat diberikan kepada unit kerja dan tim khusus.
 - f) Kriteria penamaan akun *e-mail* dinas kedinasan untuk ASN meliputi:
 - (1) Disesuaikan dengan nama asli sesuai data kepegawaian.
 - (2) Setiap kata dari nama harus dipisah menggunakan karakter titik (dot), contoh: nama.pegawai@anri.go.id.
 - (3) Apabila terdapat ASN dengan nama yang sama, maka akun *e-mail* dinas masing-masing ASN harus ditambahkan nomor urut yang berbeda, contoh: nama.pegawai1@anri.go.id dan nama.pegawai2@anri.go.id
 - g) Kriteria penamaan akun *e-mail* dinas kedinasan untuk unit kerja dan tim khusus meliputi:
 - (1) Disesuaikan dengan akronim atau singkatan dari nama unit kerja/tim khusus, contoh: pusdatinjastek@anri.go.id.
 - (2) Setiap akronim atau singkatan dari unit kerja/tim khusus harus dipisah menggunakan karakter titik (dot), contoh: sekretariat.utama@anri.go.id.
 - h) Panjang minimal karakter kata sandi pada *e-mail* dinas adalah 8 (delapan) karakter, menggunakan kombinasi huruf dan angka, sedapat mungkin menggunakan spesial karakter (seperti: 1\$%#*).

- i) *E-mail* dinas hanya digunakan untuk tujuan pekerjaan, operasional, dan kepentingan layanan ANRI.
- j) *E-mail* dinas digunakan sebagai surat resmi ANRI, untuk komunikasi pekerjaan dan untuk mendistribusikan buletin/berita yang berhubungan dengan pekerjaan.
- k) *E-mail* dinas menggunakan domain @anri.go.id.
- l) *E-mail* dinas dapat diakses pada tautan <https://mail.anri.go.id>.
- m) Penggunaan *e-mail* dinas tidak diperbolehkan untuk kegiatan-kegiatan berikut:
 - (1) Pembahasan hal yang berkaitan dengan kegiatan politik atau isu politik.
 - (2) Pengumpulan dan pengiriman pesan yang isinya bertentangan dengan hukum, sosial, aturan agama, dan kode etik, termasuk ancaman, diskriminasi, intimidasi, lelucon, pelecehan, pencemaran nama baik, pornografi, provokasi, mendiskreditkan suku, agama ras dan sosial kelas.
 - (3) Pengiriman pesan yang berasal dari sumber yang tidak dapat dipertanggungjawabkan kebenarannya, seperti surat kaleng.
 - (4) Pengiriman pesan untuk keuntungan pribadi.
 - (5) Pengambilan dan pengiriman pesan dalam sebuah *file* yang tidak terkait dengan kepentingan ANRI.
 - (6) Penyebaran informasi elektronik ke sistem *e-mail* pengguna untuk hal-hal yang tidak berhubungan dengan kegiatan ANRI.
- n) Daftar penerima (*To*, *Cc*, dan *Bcc*), *subject*, lampiran dan/atau konten *e-mail* sepenuhnya menjadi tanggung jawab pengirim.
- o) Setiap ASN ANRI tidak diperkenankan untuk membuka atau mengirimkan *e-mail* yang tidak diketahui dan/atau diduga/dianggap *virus/spam/junk e-mail* kepada pengguna *e-mail* lain. Jika menemukan hal-hal tersebut, setiap ASN wajib menghapus segera *e-mail* tersebut.

- p) Setiap pengiriman atau penerimaan lampiran *file* harus didahului dengan melakukan *scanning*.
- q) Harus dilakukan kompresi untuk lampiran *file* dengan ukuran besar sebelum dikirimkan.
- r) Beberapa jenis *file* (misalnya: *bat.*, *cmd.*, *file* multimedia, dan lain- lain) tidak diperbolehkan untuk dijadikan sebagai lampiran *e-mail*.
- s) Penulisan *disclaimer e-mail* yang akan dikirimkan harus mencakup beberapa hal sebagai berikut:
 - (1) *Disclaimer* harus mencantumkan klausul mengenai keamanan informasi.
 - (2) *Disclaimer* harus menginformasikan bahwa informasi yang terkandung dalam *e-mail* adalah milik ANRI.
 - (3) *Disclaimer* harus mencantumkan klausul mengenai langkah yang harus dilakukan apabila penerima *e-mail* bukanlah sebagaimana yang dimaksud oleh pengirim.
 - (4) *Disclaimer* mencantumkan pelarangan bagi yang tidak berhak (penerima *e-mail* bukanlah sebagaimana yang dimaksud oleh pengirim) untuk membaca, mendistribusikan dan/atau menduplikasikan informasi yang terkandung dalam *e-mail* yang diterima.
- t) Setiap *e-mail* yang tersimpan dalam kotak masuk *e-mail* memiliki masa aktif. Penyedia layanan tidak bertanggung jawab atas segala sesuatu terkait dengan penghapusan *e-mail*.
- u) Setiap mengirim *e-mail* (*send*), mengirim balik (*reply*) atau meneruskan (*forward*) harus mencantumkan nama pengirim dan *subject* harus mencerminkan isi *e-mail*, serta format penulisan isi mengikuti ketentuan penulisan surat dinas ANRI.
- v) Dilarang mengubah, mengurangi maupun menambahkan sesuatu sehingga berbeda dengan *e-mail* asli, pada saat mengirim balik (*reply*) atau meneruskan (*forward*) *e-mail*.
- w) Dilarang mengirim balik (*reply*),

meneruskan/menyebarakan (*forward*) suatu *e-mail* berantai, iklan, *spam*, *phising*, *bulk*, *hoax* atau *e-mail* yang berisi virus, *worm*, *trojan*, *spyware*, *rootkit* atau program jahat lain.

- x) Dilarang mengirim balik ke semua (*reply all*) jika materi *e-mail* yang dikirim tidak berhubungan langsung dengan *all recipient*.
- y) Seluruh *e-mail* yang dibuat, disimpan, dikirim atau diterima ASN melalui sistem *e-mail* adalah milik ANRI.
- z) ANRI berhak melakukan pengecekan atau membuka *e-mail* yang keluar atau masuk ke dalam sistem tanpa pemberitahuan sebelumnya.
- aa) ANRI berhak untuk mengumpulkan, menyimpan, menggunakan atau mengungkapkan informasi elektronik pribadi, dalam rangka penyelidikan atau penegakan hukum, dan hanya dapat diajukan oleh unit internal audit.
- bb) Pembuatan baru, perubahan akun dan penambahan kuota kapasitas simpan *mailbox e-mail* dinas diajukan secara tertulis oleh unit kerja kepada unit kerja yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi.
- cc) Proses *reset* kata sandi *e-mail* dinas bagi ASN, unit kerja dan tim khusus dapat diajukan secara tertulis oleh ASN, unit kerja dan tim khusus kepada unit kerja yang melaksanakan
- dd) tugas dan fungsi di bidang teknologi informasi dan komunikasi atau dapat diajukan melalui layanan helpdesk TIK pada tautan <https://helpdesk.anri.go.id/>.
- ee) *E-mail* dinas bagi ASN akan dinonaktifkan secara permanen (*permanently deactivated*) oleh unit kerja yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi apabila ASN sudah tidak bekerja di ANRI.

4) Pengelolaan Data Pribadi

a) Pemrolehan dan Pengumpulan Data Pribadi

- (1) Data pribadi hanya dapat diperoleh dan dikumpulkan untuk keperluan yang sah, jelas, dan terbatas pada tujuan tertentu sesuai dengan tugas dan fungsi ANRI.
- (2) Pemerolehan dilakukan secara langsung dari subjek data pribadi atau melalui pihak ketiga yang sah, dengan persetujuan eksplisit dari subjek data.
- (3) ANRI wajib menyampaikan pemberitahuan kepada subjek data pribadi mengenai : Identitas Pengendali Data, Tujuan Pemrosesan Data, Jenis Data yang dikumpulkan, Jangka Waktu Penyimpanan, dan Hak-hak Subjek Data Pribadi.
- (4) ANRI memberikan akses dan salinan Data Pribadi kepada Subjek Data Pribadi berdasarkan permintaan yang sah, setelah dilakukan verifikasi identitas, sesuai dengan ketentuan peraturan perundang-undangan.

b) Pengolahan dan Penganalisan

- (1) Pengolahan data pribadi dilakukan secara terbatas sesuai dengan tujuan pengumpulan dan atas dasar persetujuan subjek data, kecuali ditentukan lain oleh peraturan perundang-undangan.
- (2) Setiap proses pengolahan wajib mempertimbangkan prinsip minimalisasi data dan akurasi.
- (3) Penganalisan data tidak boleh dilakukan untuk tujuan diskriminatif atau yang melanggar hukum.
- (4) Pengolahan harus dicatat dalam log aktivitas data pribadi oleh unit pengelola.

c) Penyimpanan

- (1) Data pribadi disimpan dalam sistem elektronik atau non- elektronik dengan keamanan yang sesuai standar perlindungan data pribadi.
- (2) Penyimpanan dilakukan selama data tersebut masih dibutuhkan untuk kepentingan ANRI atau berdasarkan ketentuan retensi arsip yang berlaku.

- (3) Sistem penyimpanan harus menjamin: Kerahasiaan data, keutuhan data, Ketersediaan untuk akses yang sah.

d) Perbaikan dan Pembaruan

- (1) Subjek data pribadi memiliki hak untuk meminta koreksi, pembaruan, atau penyempurnaan data pribadi yang tidak akurat atau tidak lengkap.
- (2) ANRI wajib memberikan mekanisme yang mudah dan aman bagi subjek data untuk melakukan permintaan tersebut.
- (3) Koreksi atau pembaruan harus diselesaikan dalam jangka waktu maksimal 14 (empat belas) hari kerja sejak diterimanya permintaan.
- (4) Proses pembaruan wajib didokumentasikan oleh unit pengelola.

e) Penampilan, Pengumuman, Transfer, Penyebarluasan, atau Pengungkapan

- (1) Penampilan atau pengungkapan data pribadi hanya boleh dilakukan atas dasar:
 - Persetujuan eksplisit dari subjek data,
 - Perintah undang-undang, atau
 - Putusan pengadilan yang berkekuatan hukum tetap.
- (2) Transfer atau penyebarluasan data ke pihak lain, termasuk lintas instansi, hanya diperbolehkan jika:
 - Terdapat perjanjian pemrosesan data,
 - Data telah melalui proses minimalisasi dan keamanan,
 - Pihak penerima memiliki standar perlindungan data yang setara.
- (3) Pengungkapan ke publik dilarang, kecuali data tersebut telah dianonimkan atau diubah bentuknya sehingga tidak dapat diidentifikasi lagi secara pribadi.

f) Penghapusan atau Pemusnahan

- (1) Data pribadi wajib dihapus atau dimusnahkan apabila:

- 1) Tujuan pengumpulan dan/atau pemrosesan telah tercapai;
 - 2) Masa retensi telah berakhir berdasarkan JRA dan penilaian pemusnahan.
 - 3) Subjek data mencabut persetujuan dan tidak ada dasar hukum lain untuk pemrosesan data;
 - 4) Berdasarkan perintah pengadilan.
- (2) Penghapusan atau pemusnahan harus dilakukan secara aman agar data tidak dapat dipulihkan kembali.
- (3) Proses penghapusan wajib dicatat dan dilaporkan oleh unit pengelola, serta didokumentasikan sebagai bagian dari audit data pribadi.

g) Tata Kelola Pelindungan Data Pribadi.

Dalam rangka memastikan pemrosesan data pribadi dilakukan secara sah, aman, akuntabel, dan sesuai dengan ketentuan peraturan perundang-undangan mengenai pelindungan data pribadi, ANRI menetapkan tata kelola pelindungan data pribadi dalam pelaksanaan Sistem Manajemen Keamanan Informasi.

Tata kelola pelindungan data pribadi sebagaimana dimaksud paling sedikit mencakup:

1. penetapan pejabat atau petugas yang melaksanakan fungsi pelindungan data pribadi dan Lembaga Pelaksana Audit Teknologi Informasi dan Komunikasi (LATIK) sesuai dengan ketentuan peraturan perundang-undangan;
2. pelaksanaan Risk Impact Assessment (RIA) atau penilaian risiko dan dampak atas aktivitas pemrosesan data pribadi;
3. pelaksanaan Data Protection Impact Assessment (DPIA) atau penilaian dampak pelindungan data pribadi terhadap pemrosesan data pribadi yang berisiko tinggi;
4. penyusunan dan pemutakhiran Record of Processing Activities (ROPA) atau catatan

aktivitas pemrosesan data pribadi;

5. pengelolaan dasar pemrosesan data pribadi, tujuan pemrosesan, kategori data pribadi, subjek data pribadi, penerima data pribadi, jangka waktu penyimpanan, media penyimpanan, lokasi pemrosesan, dan kontrol keamanan yang diterapkan;
6. pemantauan kepatuhan terhadap pemenuhan hak subjek data pribadi; dan
7. pelaporan, evaluasi, dan tindak lanjut terhadap risiko, insiden, atau pelanggaran perlindungan data pribadi.

Pejabat atau petugas yang melaksanakan fungsi perlindungan data pribadi sebagaimana dimaksud bertugas memberikan saran dan rekomendasi terkait kepatuhan perlindungan data pribadi, memantau pelaksanaan kebijakan dan prosedur perlindungan data pribadi, memberikan masukan atas *Rich Internet Application (RIA)*, *Data Protection Impact Assessment (DPIA)*, dan *Record of Processing Activities (RoPA)*, serta berkoordinasi dengan unit kerja pemilik data, unit kerja pemilik proses bisnis, unit kerja yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi, dan unit kerja terkait lainnya.

RIA dan DPIA dilakukan sebelum dan/atau pada saat terdapat pemrosesan data pribadi baru, perubahan proses bisnis, pengembangan atau perubahan aplikasi, penggunaan teknologi baru, integrasi data, transfer data kepada pihak lain, atau pemrosesan data pribadi yang berpotensi menimbulkan risiko tinggi bagi subjek data pribadi.

RoPA disusun dan dimutakhirkan secara berkala dan/atau sewaktu-waktu apabila terdapat perubahan aktivitas pemrosesan data pribadi, perubahan regulasi, perubahan sistem elektronik, perubahan tujuan pemrosesan, perubahan pihak penerima data, hasil audit, hasil evaluasi, atau insiden perlindungan

data pribadi.

Penanggung jawab pelaksanaan tata kelola perlindungan data pribadi adalah unit kerja pemilik data dan/atau pemilik proses bisnis bersama unit kerja yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi serta pejabat atau petugas yang melaksanakan fungsi perlindungan data pribadi sesuai dengan kewenangannya

5) Perjanjian Kerahasiaan

- a) Setiap pegawai maupun pihak ketiga harus menyetujui dan menandatangani pernyataan menjaga kerahasiaan informasi yang dituangkan dalam dokumen pernyataan kerahasiaan informasi atau kontrak kerja dan berlaku selama personel aktif bekerja di ANRI.
- b) Perjanjian kerahasiaan harus dibuat dan disetujui secara formal melalui proses penandatanganan oleh seluruh pihak baik internal maupun eksternal yang mengakses informasi maupun sistem informasi ANRI yang tidak bersifat publik.
- c) Perjanjian kerahasiaan secara hukum mendukung perlindungan informasi dan sistem informasi ANRI dari risiko pengungkapan (*disclosure*) tanpa izin.
- d) Dalam penyusunan perjanjian kerahasiaan perlu mempertimbangkan beberapa aspek berikut:
 - (1) Pendefinisian dan identifikasi dari informasi yang perlu dilindungi.
 - (2) Durasi/masa berlakunya perjanjian kerahasiaan, hal ini perlu mempertimbangkan sensitivitas dan masa retensi dari informasi dan sistem informasi yang terkait.
 - (3) Tanggung jawab dan tindakan yang harus diambil pihak yang menandatangani perjanjian untuk menghindari pengungkapan (*disclosure*) informasi tanpa izin.
 - (4) Kepemilikan dari informasi, rahasia dan kekayaan intelektual, berhubungan dengan perlindungan dari kerahasiaan informasi tersebut.
 - (5) Panduan mengenai bagaimana informasi rahasia

boleh digunakan.

- (6) Hak untuk melakukan audit dan memantau aktivitas penanda tangan perjanjian.
 - (7) Proses pemberitahuan dan pelaporan apabila terjadi pengungkapan tanpa izin atau kebocoran informasi.
 - (8) Tindakan yang akan dilakukan apabila terjadi pelanggaran perjanjian.
 - (9) Perjanjian harus sesuai dengan ketentuan peraturan perundang-undangan.
- e) Penanggung Jawab Pengelolaan Pertukaran Informasi
Penanggung jawab pengelolaan pertukaran informasi adalah unit kerja yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi.
- c. Pengelolaan Keamanan Informasi dalam Hubungan dengan Pihak Ketiga
- 1) Aturan Keamanan Informasi untuk Pihak Ketiga
 - a) Proses keamanan informasi terkait dengan akses pihak ketiga untuk aset ANRI harus disepakati dengan pihak ketiga.
 - b) Seluruh mitra selaku pihak ketiga harus diidentifikasi dan didokumentasikan. Dokumentasi harus mencakup informasi terkait pihak ketiga, layanan yang diberikan serta referensi ke kontrak kerja.
 - c) Pemilihan pihak ketiga harus mengikuti ketentuan kriteria sesuai dengan Peraturan Pengadaan Barang dan Jasa Instansi Pemerintah;
 - d) Setiap kontrak kerja antara ANRI dan pihak ketiga harus mencakup:
 - (1) Perjanjian kerahasiaan.
 - (2) Prasyarat untuk mengikuti persyaratan keamanan informasi ANRI.
 - (3) Tanggung jawab dari kedua belah pihak.
 - (4) Jika penyediaan layanan oleh pihak ketiga melibatkan subkontraktor, pihak ketiga harus memberikan kepastian bahwa persyaratan keamanan elektronik akan diikuti oleh para subkontraktor.

- e) Akses ke informasi dan aset *data center* yang dilakukan oleh pihak ketiga harus diberikan berdasarkan kebutuhan dan disetujui oleh ANRI.
 - f) Personel pihak ketiga harus diberikan informasi terkait prasyarat keamanan informasi dan harus menandatangani perjanjian kerahasiaan.
 - g) Kewajiban pihak ketiga dan tingkat layanan harus ditetapkan secara formal dalam kontrak kerja.
 - h) Metode komunikasi antara ANRI dan pihak ketiga harus ditetapkan terutama terkait penanganan insiden.
- 2) Menangani Keamanan Informasi dalam Perjanjian dengan Pihak Ketiga
- a) Perjanjian dengan pihak ketiga harus mencakup klausul kerahasiaan informasi yang disetujui oleh pihak ketiga.
 - b) Setiap personel pihak ketiga yang dapat mengakses, memproses, menyimpan, berkomunikasi, atau mengkonfigurasi komponen infrastruktur teknologi informasi dan komunikasi, dan informasi untuk ANRI harus menandatangani perjanjian kerahasiaan informasi.
- 3) Penanggung Jawab Pengelolaan Keamanan Informasi dalam Hubungan dengan Pihak Ketiga.
- Penanggung jawab pengelolaan keamanan informasi dalam hubungan dengan pihak ketiga adalah masing-masing unit kerja yang menyelenggarakan kerja sama dengan pihak ketiga di ANRI.
- d. Pengelolaan Media Penyimpanan Informasi Pengelolaan Media Penyimpanan Informasi mencakup hal-hal:
- 1) Pengelolaan *Removable Media*
 - a) Yang digolongkan sebagai *removable media* antara lain *external hardisk*, *USB flash disk* dan *memory card*.
 - b) *Removable media* yang digunakan di ANRI perlu dicatat, didokumentasikan apabila terdapat perubahan, dan perangkat yang digunakan mempunyai fitur keamanan yang memadai.
 - c) Data yang tersimpan di dalam *removable media* yang

tidak akan digunakan kembali harus dihapus secara permanen dan dipastikan tidak dapat di-*recover*.

- d) Pegawai harus selalu melakukan *scanning* virus terhadap *removable* media (*flash disk*, *external harddisk*) untuk mencegah adanya kerusakan informasi akibat *malware*.
- e) Seluruh *removable* media harus disimpan di tempat dan lingkungan yang aman.
- f) *Removable* media yang tidak boleh digunakan untuk menyimpan informasi yang bersifat rahasia adalah *external hardisk*, *USB flash disk*, dan *memory card*.
- g) Seluruh unit kerja bertanggung jawab terhadap pengelolaan *removable* media yang digunakan untuk menyimpan informasi ANRI.

- 2) Pemindahan media secara elektronik media yang menyimpan informasi milik ANRI harus dilindungi dari akses tanpa izin, modifikasi dan penyalahgunaan selama dalam proses pemindahan dari area ANRI.

3. Pencegahan Kebocoran Data

Pencegahan kebocoran data/*Data Loss Prevention* (DLP) adalah pengendalian keamanan yang dirancang untuk mencegah kehilangan, kebocoran, atau penggunaan tidak sah data sensitif oleh pihak yang tidak berwenang. Mekanisme DLP melibatkan penggunaan kebijakan, teknologi, dan proses untuk mengidentifikasi, melindungi, dan mengendalikan data sensitif.

- a. Identifikasi data sensitif yang perlu dilindungi melalui mekanisme klasifikasi informasi. Informasi tersebut termasuk data pribadi dan informasi rahasia ANRI.
- b. Penetapan kebijakan DLP menjelaskan jenis data yang dianggap sensitif, aturan penggunaan dan distribusi data sensitif, serta konsekuensi dari pelanggaran kebijakan. Kebijakan DLP harus mencakup penggunaan data di ANRI serta pengiriman data melalui jaringan internal dan eksternal.
- c. Identifikasi dan pengawasan data menggunakan teknologi DLP untuk mengidentifikasi dan memonitor data sensitif. Teknologi DLP dapat memindai data dalam berbagai bentuk seperti dokumen, *e-mail*, pesan instan, atau data yang

dipindahkan melalui jaringan. DLP dapat mengenali pola atau tanda-tanda khusus yang mengindikasikan data sensitif, seperti nomor kartu kredit, nomor rekening bank, atau informasi pribadi lainnya.

d. Pendefinisian Metadata Data Sensitif dan Aturan Pendeteksian DLP.

Dalam rangka meningkatkan efektivitas pencegahan kebocoran data, ANRI menetapkan metadata data sensitif dan aturan pendeteksian pada mekanisme DLP.

Metadata data sensitif sebagaimana dimaksud merupakan informasi pendukung yang digunakan untuk mengidentifikasi, mengklasifikasikan, melacak, dan melindungi data sensitif dan/atau data pribadi yang dikelola oleh ANRI. Metadata data sensitif paling sedikit mencakup jenis data, klasifikasi informasi, pemilik data, sumber data, lokasi penyimpanan, format atau struktur data, tingkat risiko, dasar pemrosesan, masa retensi, media atau kanal pertukaran data, serta kontrol pengamanan yang diterapkan.

Aturan pendeteksian DLP sebagaimana dimaksud ditetapkan untuk mengenali pola, karakteristik, kata kunci, format, struktur, atau tanda khusus yang mengindikasikan keberadaan data sensitif dan/atau data pribadi, termasuk namun tidak terbatas pada data identitas, data kepegawaian, data keuangan, data kesehatan, kredensial akses, dokumen rahasia, informasi strategis, dan data lain yang diklasifikasikan sebagai terbatas, rahasia, atau sangat rahasia.

Aturan pendeteksian DLP diterapkan pada media dan kanal yang relevan, paling sedikit meliputi dokumen elektronik, surat elektronik, pesan instan, penyimpanan berbagi, perangkat endpoint, removable media, aplikasi, basis data, serta lalu lintas data pada jaringan internal maupun eksternal.

Hasil pendeteksian DLP digunakan sebagai dasar untuk pemberian peringatan, pembatasan, pemblokiran, karantina, pencatatan, pelaporan, investigasi, serta tindak lanjut terhadap dugaan kehilangan, kebocoran, penyalahgunaan, atau pengiriman data sensitif dan/atau data pribadi kepada

pihak yang tidak berwenang.

Metadata data sensitif dan aturan pendeteksian DLP dilakukan revidi dan pemutakhiran secara berkala dan/atau sewaktu-waktu apabila terdapat perubahan klasifikasi informasi, perubahan proses bisnis, perubahan regulasi, hasil audit, hasil evaluasi, insiden keamanan informasi, atau perkembangan ancaman keamanan siber.

Penanggung jawab pendefinisian metadata data sensitif dan aturan pendeteksian DLP adalah unit kerja yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi bersama unit kerja pemilik data dan/atau pemilik proses bisnis.

- e. Kontrol dan pencegahan yang diperlukan untuk melindungi data sensitif. Contohnya, penggunaan enkripsi untuk data yang dikirim melalui jaringan, pembatasan akses berdasarkan peran dan tanggung jawab, atau penandaan otomatis data sensitif. Mekanisme DLP juga dapat memblokir atau menghapus data yang dianggap melanggar kebijakan DLP.
- f. Mekanisme pelaporan yang memungkinkan identifikasi pelanggaran kebijakan DLP. Ketika ada pelanggaran yang terdeteksi, langkah-langkah tindak lanjut yang sesuai harus diambil. Tindak lanjut dapat meliputi penyelidikan internal, pelaporan kepada otoritas yang berwenang, atau tindakan disiplin berdasarkan peraturan dan regulasi.
- g. Program pelatihan dan kesadaran untuk pegawai tentang kebijakan DLP dan implementasi penggunaan data yang aman. Pegawai diberikan pemahaman tentang jenis data sensitif, konsekuensi pelanggaran kebijakan, dan langkah-langkah yang harus diambil untuk melindungi data.

4. *Data Masking*

Metode *data masking* merupakan pendekatan untuk melindungi data sensitif dengan menggantinya dengan data yang serupa namun tidak dapat diidentifikasi secara langsung. Metode ini digunakan untuk mengurangi risiko kebocoran data dan memastikan bahwa data sensitif hanya dapat diakses oleh pihak yang berwenang. Penggunaan enkripsi dapat digunakan untuk memberikan perlindungan ganda pada data yang bersifat sensitif.

- a. Identifikasi data sensitif merupakan langkah pertama untuk

mengidentifikasi jenis data sensitif yang perlu dilindungi, seperti nomor kartu kredit, data medis, atau informasi identifikasi pribadi. Hal ini penting untuk memahami jenis data yang harus di-mask dan melindunginya dengan tepat.

- b. Penentuan metode *data masking* yang sesuai harus ditentukan. Metode yang digunakan meliputi:
 - 1) Substitusi Karakter, yaitu karakter dalam data sensitif diganti dengan karakter lain yang tidak memiliki arti atau relevansi. Misalnya, nomor kartu kredit dapat digantikan dengan karakter 'X' atau 'Y'.
 - 2) Pertukaran Nilai, yaitu nilai dalam data sensitif ditukar dengan nilai yang serupa namun tidak dapat dihubungkan secara langsung ke data asli. Contohnya, tanggal lahir dapat digantikan dengan tanggal acak pada tahun yang sama.
 - 3) Pembuatan Data Palsu, yaitu data palsu yang tidak berhubungan dengan data asli dapat dibuat untuk menggantikan data sensitif. Namun, penting untuk memastikan bahwa data palsu tersebut memiliki karakteristik yang mirip dengan data asli.
- c. Implementasi *data masking* diterapkan pada data yang bersifat sensitif. Hal ini dapat melibatkan penggunaan algoritma dan proses lainnya untuk menggantikan data asli dengan data yang telah dilakukan proses data masking.

5. *Threat Intelligence*

- a. *Threat intelligence* berfokus pada pengumpulan, analisis, dan penggunaan informasi untuk melindungi ANRI dari ancaman keamanan dan menjadi lebih responsif terhadap serangan yang berpotensi merugikan dan meminimalkan dampak negatif.
- b. Metode pengumpulan data yang digunakan dapat melibatkan pemanfaatan sumber daya internal dan eksternal, seperti sistem monitoring, sumber terbuka, grup keamanan, atau pihak ketiga penyedia layanan *threat intelligence*.
- c. Pertukaran informasi ancaman dan kerentanan dengan BSSN, *Gov- Computer Security Incident Response Team* CSIRT, instansi terkait, dan/atau komunitas tepercaya dilaksanakan melalui Tim Tanggap Insiden Siber ANRI (TTIS ANRI) dengan

memperhatikan klasifikasi informasi, kebutuhan untuk mengetahui, kerahasiaan, dan ketentuan peraturan perundang-undangan.

- d. Data *threat intelligence* akan dianalisis dan dievaluasi yang mencakup identifikasi ancaman yang relevan, pemahaman mengenai metode serangan yang digunakan, dan penilaian tingkat risiko yang terkait dengan ancaman tersebut.
- e. Informasi *threat intelligence* yang relevan dikomunikasikan kepada pemangku kepentingan di ANRI. Informasi tersebut dapat mencakup taktik, teknik, dan prosedur yang digunakan oleh penyerang, serta langkah-langkah yang harus diambil untuk mencegah serangan atau merespons serangan yang sedang berlangsung.
- f. Tindakan yang diambil dalam merespon ancaman yang terdeteksi melibatkan kegiatan pemantauan, pelaporan insiden keamanan, serta prosedur respon insiden dan keberlangsungan bisnis.

B. Infrastruktur Teknologi Informasi dan Komunikasi

Infrastruktur teknologi informasi dan komunikasi mencakup seluruh perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat elektronik lainnya.

1. Pengelolaan Aset Teknologi Informasi Komunikasi

Standar pengelolaan aset mencakup hal-hal sebagai berikut:

a. Inventarisasi Aset

- 1) Inventarisasi aset teknologi informasi komunikasi ANRI meliputi:

- a) Perangkat lunak dan aplikasi.
- b) Aset fisik yang meliputi PC, *notebook*, *server*, *removable media*, *printer*, dan *scanner*.
- c) Perangkat jaringan, layanan jaringan, dan keamanan jaringan.
- d) Sarana maupun layanan pendukung seperti, genset, *Uninterrupted Power Supply* (UPS), dan *Air Conditioner* (AC),
- e) Layanan Pihak Ketiga.

- 2) Daftar inventarisasi aset teknologi informasi komunikasi harus diperiksa kesesuaiannya dengan kondisi nyata dan dilakukan pembaruan setiap ada perubahan.
 - 3) Penanggung jawab inventarisasi aset fisik adalah unit kerja yang memiliki tugas melaksanakan pengelolaan dan pemanfaatan barang milik negara di lingkungan ANRI.
 - 4) Penanggung jawab inventarisasi aplikasi, jaringan dan informasi adalah unit kerja pemilik informasi.
- b. Ketentuan Penanggung Jawab Aset
- 1) Penetapan penanggung jawab aset bagi setiap aset teknologi informasi komunikasi yang digunakan di lingkungan ANRI, yang ditujukan untuk:
 - a) Memastikan aset telah diklasifikasikan dan diamankan dengan baik.
 - b) Menentukan hak akses ke aset tersebut.
 - c) Melakukan peninjauan terhadap klasifikasi dan pengamanan aset secara periodik.
 - 2) Pemeliharaan aset menjadi tanggung jawab dari pemilik aset tersebut.
- c. Standar Penggunaan Aset
- 1) Semua perangkat teknologi informasi komunikasi yang digunakan merupakan perangkat milik ANRI dan hanya untuk kepentingan pekerjaan.
 - 2) Penggunaan perangkat pribadi untuk mengakses sistem layanan jaringan ANRI harus mendapatkan persetujuan pejabat terkait di ANRI.
 - 3) Aturan penggunaan layanan jaringan bagi pegawai ANRI disetujui oleh pimpinan tinggi pratama yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi selaku Pejabat Sistem Keamanan Informasi.
 - 4) Aturan penggunaan informasi dan aset pemrosesan informasi disetujui oleh pimpinan tinggi pratama yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi selaku Pejabat Sistem Keamanan Informasi.
 - 5) Semua pengguna baik pegawai ANRI maupun pihak ketiga harus mematuhi peraturan yang berlaku. Peraturan

tersebut mencakup namun tidak terbatas pada:

- a) Aturan mengenai *e-mail* dan penggunaan *internet*.
- b) Pedoman penggunaan *mobile device*, khususnya penggunaan *device* di luar lingkungan kantor.
- 6) Seluruh pegawai maupun pihak ketiga harus memiliki kesadaran (*awareness*) mengenai aturan penggunaan aset dan tanggung jawab keamanan informasi terkait dengan penggunaan aset tersebut.

d. Pengembalian Aset

- 1) Setiap pegawai yang sudah tidak bekerja, pensiun, dan pindah kerja dalam/luar instansi ANRI harus mengembalikan aset teknologi informasi komunikasi beserta seluruh informasi milik ANRI yang sudah bukan menjadi kewenangannya.
- 2) Aset yang dimaksud mencakup perangkat keras dan perangkat lunak pengolahan informasi beserta seluruh informasi yang terdapat di dalamnya.
- 3) Pengembalian aset teknologi informasi komunikasi dilakukan secara formal dan terdokumentasi sesuai dengan ketentuan yang berlaku.
- 4) Penanggung jawab pengembalian aset adalah masing-masing unit kerja yang mengelola aset teknologi informasi dan komunikasi di ANRI.

2. Keamanan Fisik dan Lingkungan

I. Pengelolaan Wilayah yang Aman

Prosedur pengelolaan wilayah yang aman mencakup:

a. Pembagian Area

Area di lingkungan ANRI dibagi menjadi 2 (dua), yaitu:

1) Area Terbatas

Area terbatas merupakan area yang dapat diakses oleh pihak yang berwenang, yaitu pegawai, pihak ketiga yang memiliki hubungan pekerjaan dengan ANRI, serta pihak yang memiliki kepentingan bisnis maupun operasional dengan ANRI. Area yang dikategorikan sebagai area terbatas di lingkungan ANRI mencakup:

- a) Ruang kerja pegawai.
- b) Ruang rapat.
- c) Area ANRI selain yang masuk dalam kategori area

keamanan khusus.

2) Area Keamanan Khusus

Area keamanan khusus merupakan area yang di dalamnya terdapat informasi dan fasilitas yang bersifat kritikal yang perlu dilindungi dari akses tanpa izin, kerusakan dan gangguan. Area yang dikategorikan sebagai keamanan khusus di ANRI mencakup:

a) Pusat Data (*Data Center*);

Pusat Data/*Data Center* adalah suatu area/ruangan yang terdiri atas ruang *server* dan ruangan-ruangan lain yang diperlukan untuk mendukung kerja *server* serta memantau kinerja *server*. Suatu ruangan yang digunakan untuk menempatkan sistem komputer/*server* dan komponen-komponen terkait seperti sistem telekomunikasi atau pusat jaringan dan penyimpanan data.

b) Pusat Pemulihan Bencana (*Disaster Recovery Center*) Pusat Pemulihan Bencana adalah pusat data yang dirancang khusus untuk memulihkan data dan sistem di ANRI yang terganggu apabila terjadi bencana alam atau gangguan teknis lainnya.

c) *Security Operation Center* (SOC)

Security Operation Center adalah pusat operasi yang didedikasikan untuk memantau dan mengelola keamanan informasi serta infrastruktur teknologi informasi dan komunikasi ANRI.

d) *Network Operation Center* (NOC)

Network Operation Center adalah ruang yang digunakan untuk memantau kondisi dan kinerja jaringan komunikasi dan memantau kondisi lingkungan *data center*. Di dalam ruang NOC umumnya terdapat *server-server access control*, *Closed Circuit Television* (CCTV) dan *environmental management system* yang digunakan memantau suhu dan kelembaban di *data center*.

e) Area tempat penyimpanan fasilitas pendukung dari

aset teknologi informasi *tersebut*, sebagai contoh ruang penyimpanan instalasi pendingin udara, generator, UPS serta panel listrik.

b. Pengelolaan Perimeter Keamanan Fisik

- 1) Pembatasan wilayah dengan pembatas secara fisik harus diterapkan untuk melindungi area yang berisi informasi dan/atau fasilitas pengolahan informasi.
- 2) Pengamanan fisik ruangan di lingkungan ANRI mengacu kepada klasifikasi wilayah masing-masing ruangan dengan menggunakan pembatas dan pengendalian akses fisik, berupa kartu kontrol akses, fingerprint, PIN).
- 3) Pembatasan akses ke dalam area ANRI antara lain dengan membuat daerah penerimaan tamu yang dijaga atau melengkapi pintu dan jendela dengan kunci secara fisik maupun elektronik untuk menjamin akses hanya untuk personel yang berkepentingan.
- 4) Pemantauan akses ke dalam area ANRI untuk mendeteksi aktivitas yang dapat menimbulkan kerugian ANRI.
- 5) Penempatan fasilitas pemrosesan informasi di dalam ruangan yang memiliki kontrol pengamanan akses keluar masuk yang memadai.
- 6) Pemisahan secara fisik antara fasilitas pemrosesan informasi ANRI dengan area kerja pihak ketiga.
- 7) Pemasangan sistem alarm yang terpantau pada pintu darurat dan sistem alarm tersebut harus diuji secara berkala.

c. Pengendalian Akses Fisik Area Keamanan Khusus

- 1) Pengendalian akses fisik area keamanan khusus untuk menjamin tidak adanya akses tanpa izin.
- 2) Pencatatan atas tamu atau pihak ketiga yang datang ke area keamanan khusus di lingkungan ANRI termasuk pencatatan tanggal dan waktu masuk maupun keluarnya.
- 3) Pendampingan dan pengawasan kepada tamu atau pihak ketiga selama berada di area khusus kecuali

telah mendapatkan izin akses.

- 4) Penyampaian informasi kepada pengunjung area khusus mengenai syarat keamanan area keamanan khusus beserta prosedurnya dalam keadaan darurat.
- 5) Tamu atau pihak ketiga yang diizinkan untuk mengakses area kritikal di ANRI hanya pegawai yang mempunyai kewenangannya dan diotorisasi oleh pejabat penanggung jawab di ruang tersebut dan harus diawasi dan didampingi oleh pegawai di ruangan tersebut.
- 6) Pengendalian akses masuk kedalam area tempat pemrosesan/penyimpanan informasi sensitif dengan menggunakan *dual authentication* seperti kombinasi *fingerprint*, kartu Akses atau *personal identification number*. Audit trail terkait akses ke dalam area tersebut harus dikelola dengan baik.
- 7) Pegawai, Tamu atau Pihak Ketiga dilarang mengambil gambar, merekam suara atau video, atau melakukan dokumentasi lain di area keamanan khusus tanpa izin. Pembatasan, penitipan, atau pengendalian perangkat perekam diterapkan berdasarkan tingkat risiko dan ketentuan keamanan fisik.
- 8) Semua pengguna baik internal maupun eksternal wajib mengenakan *id card* ketika masuk ke dalam area keamanan khusus. Setiap pegawai harus segera melaporkan kepada petugas yang berwenang seandainya ditemukan pengguna yang tidak mengenakan *id card*.
- 9) Peninjauan secara rutin atas hak akses ke area keamanan khusus.

d. Pengamanan Ruang Kantor dan Fasilitasnya

- 1) Pengamanan secara memadai untuk ruangan kerja dan fasilitas di lingkungan ANRI dengan mempertimbangkan pemisahannya dari wilayah akses umum.
- 2) Informasi/petunjuk apapun tidak diperkenankan untuk dipasang atau menandai area kritikal dan/atau area keamanan khusus di ANRI.

- 3) Pemisahan area antara fasilitas yang digunakan untuk pemrosesan dan penyimpanan informasi sensitif dengan fasilitas yang digunakan untuk pekerjaan sehari-hari.
- 4) Implementasi pengamanan ruang kantor dan fasilitas kerja harus mempertimbangkan hal-hal berikut:
 - a) Perhatian perlu diberikan terhadap aspek kesehatan dan keamanan berdasarkan standar maupun regulasi yang berlaku.
 - b) Kantor, ruang kerja dan fasilitas ANRI perlu dirancang untuk meminimalisir akses oleh masyarakat umum.
- e. Perlindungan Terhadap Ancaman Eksternal dan Lingkungan Penyediaan peralatan pemadam kebakaran yang memadai pada tempat yang sesuai.
 - 1) Penyediaan kelengkapan peralatan pemadam kebakaran yang bersifat *non-liquid* pada ruangan kritikal dan/atau area keamanan khusus di ANRI.
 - 2) Perlindungan area ANRI dari risiko yang muncul dari kebakaran, banjir, gempa bumi, ledakan, dan bencana lainnya, baik disebabkan oleh alam maupun manusia.
 - 3) Perlindungan tersebut harus mempertimbangkan kondisi lingkungan sekitar area ANRI.
 - 4) Proses perlindungan terhadap ancaman eksternal dan lingkungan harus mempertimbangkan hal-hal sebagai berikut:
 - a) material yang berpotensi menimbulkan bahaya dan mudah terbakar harus disimpan di tempat yang aman dan terpisah dari ruang aktivitas kerja.
 - b) media backup harus disimpan di tempat dengan jarak yang cukup aman dari *main site* untuk menghindari kerusakan apabila terjadi bencana di *main site*.
 - c) memastikan area keamanan khusus memiliki detektor api dan asap serta pipa pembuangan air.
 - d) zat pemadam api dan sistem yang digunakan harus memperhatikan keamanan terhadap peralatan dan petugas pelaksana di dalam area teknologi

informasi.

- e) pusat data dan area yang sensitif yang berisi peralatan komputer yang kritikal dan harus dilindungi dengan sistem pendeteksi api dan sistem alarm otomatis.
 - f) pusat data harus berada pada lokasi yang lebih tinggi dengan detektor panas, asap, dan air.
 - g) sistem pendeteksi api dan sistem pemadaman harus diperiksa untuk dipastikan bahwa alat tersebut terpasang dengan benar, dan harus diperiksa secara rutin paling sedikit 1 (satu) kali setiap tahun.
 - h) lokasi-lokasi strategis harus dilengkapi dengan alat pemadam api darurat mudah untuk dijangkau. Instruksi penggunaannya harus terbaca dengan jelas.
 - i) diperlakukan larangan merokok serta membawa makan dan minum di area keamanan khusus.
- f. Pengelolaan Area Aman untuk bekerja
- 1) Pekerjaan yang dilakukan oleh pihak ketiga di area kritikal dan/atau area keamanan khusus di lingkungan ANRI harus selalu diawasi oleh personel penanggung jawab area tersebut untuk menghindari kegiatan yang tidak diinginkan.
 - 2) Setiap pegawai dan pihak ketiga dilarang merokok serta membawa makanan dan minuman ke dalam wilayah tertutup.
 - 3) Pihak ketiga yang memasuki wilayah area keamanan khusus tidak diperkenankan membawa peralatan *visual recording* (kamera dan/atau *handphone* berkamera).
 - 4) Pekerjaan di area keamanan khusus, baik yang dilakukan oleh pihak internal maupun eksternal, memerlukan perlindungan dan panduan khusus untuk mengurangi kemungkinan adanya kecelakaan, insiden atau gangguan dalam bekerja.
 - 5) Pintu masuk dan lokasi penting pada area keamanan khusus harus dilengkapi dengan kamera CCTV.

Perekam CCTV disimpan pada tempat aman, dan hasil rekaman CCTV disimpan untuk beberapa waktu tertentu.

- 6) Area keamanan khusus yang kosong harus selalu terkunci dan secara rutin dilakukan pengecekan.

g. Pengelolaan Area *Delivery* dan *Loading*

- 1) Akses masuk ke wilayah *loading* di ANRI harus diamankan untuk menghindari akses tanpa izin.
- 2) Pengamanan area *delivery* dan *loading* paling sedikit dilakukan dengan cara sebagai berikut:
 - a) Membatasi akses ke area tersebut hanya untuk personel yang telah terdaftar dan terotorisasi.
 - b) Menempatkan area *delivery* dan *loading*, sehingga untuk menjangkaunya personel yang mengakses area tersebut tidak perlu memasuki area terbatas dan tertutup ANRI.
 - c) Mengamankan pintu masuk ke area *delivery* dan *loading*.
 - d) Mendaftarkan dan memeriksa barang-barang yang datang dari luar sebelum dipindahkan ke area internal ANRI.

h. Penanggung Jawab Pengelolaan Keamanan Fisik

Penanggung jawab pengelolaan keamanan fisik adalah unit kerja yang melaksanakan tugas dan fungsi di bidang pengelolaan urusan tata usaha pimpinan, dan pengamanan di lingkungan ANRI.

II. Pengamanan Perangkat

Pengamanan perangkat ANRI mencakup:

a. Perlindungan dan Penempatan Peralatan

- 1) Perangkat pengolahan informasi yang dianggap kritikal perlu ditempatkan secara aman termasuk membatasi sudut pandang untuk mengurangi orang yang tidak berkepentingan bisa melihat informasi yang ditampilkan.
- 2) Peralatan kerja milik ANRI harus ditempatkan sedemikian rupa sehingga mengurangi risiko ancaman yang berasal dari lingkungan (api, air, debu).

- 3) Perlindungan peralatan kerja milik ANRI dilakukan dengan cara sebagai berikut:
 - a) Menempatkan peralatan kerja perlu dilakukan untuk mengurangi risiko adanya akses yang tidak perlu ke area kerja.
 - b) Menempatkan fasilitas atau peralatan pengolahan informasi yang diperlukan, sehingga mengurangi pandangan orang yang tidak berwenang, termasuk membatasi sudut pandang kepada peralatan tersebut.
 - c) Mengisolasi peralatan yang membutuhkan perlindungan khusus di lokasi khusus guna mengurangi jumlah pengamanan yang diperlukan.
 - d) Menerapkan kontrol yang memadai guna meminimalkan risiko ancaman gangguan fisik, seperti pencurian, kebakaran, ledakan gangguan dari asap, air, petir, debu, getaran, bahan kimia, gangguan terhadap pasokan listrik, Jaringan komunikasi, serta elektromagnetik dan vandalisasi.
 - e) Memantau kondisi suhu dan kelembaban dalam area keamanan khusus secara rutin.
 - f) Mengimplementasikan alat pelindung petir pada bangunan, jalur listrik maupun komunikasi.

b. Sarana Pendukung

- 1) Penyediaan, pemeliharaan dan pemeriksaan secara berkala atas seluruh sarana pendukung seperti *power supply*, *genset*, lampu darurat, dan AC guna mendukung kegiatan operasional area keamanan khusus, dalam hal ini pusat data ANRI.
- 2) Perlindungan peralatan pengolahan informasi elektronik dari kemungkinan hilangnya pasokan listrik dan gangguan lain yang disebabkan oleh gangguan pada sarana pendukung.
- 3) Penyediaan penerangan darurat guna menjamin penerangan dalam kondisi hilangnya pasokan listrik.
- 4) Penyediaan suplai listrik yang sesuai dengan kebutuhan peralatan pengolahan informasi.
- 5) Penggunaan *emergency power off switches* apabila

memungkinkan untuk mematikan peralatan pengolahan informasi secara cepat saat kondisi darurat.

- 6) Penyediaan bahan bakar generator listrik yang mencukupi kebutuhan pada saat diperlukan.
- 7) Penggunaan beberapa sumber pasokan listrik apabila memungkinkan terutama untuk peralatan pengolahan informasi yang sangat sensitif guna mengurangi kegagalan operasi pada peralatan pengolahan informasi apabila pasokan listrik yang ada terputus (*single point of failure*).
- 8) Pengelolaan sumber daya listrik di-*backup* oleh UPS dan generator, dilakukan sesuai prosedur berikut:
 - a) Pemasangan generator untuk mendukung penyediaan listrik pusat data.
 - b) Sumber daya listrik harus didukung oleh UPS atau baterai cadangan, dan harus mampu untuk mendukung kapasitas untuk periode sekurang-kurangnya 15 (lima belas) menit pada saat terjadi pemadaman listrik.
 - c) Ruang generator dan UPS harus aman dan terkunci. Kunci harus disimpan dan hanya dapat diakses oleh petugas yang ditunjuk.
 - d) Ruang generator dan UPS harus mempunyai ventilasi yang memadai dan dilengkapi dengan sistem pendeteksi dan perlindungan dari api.
- 9) Pemeliharaan dan pengetesan atas ketersediaan *power* dari generator dan UPS dilakukan secara periodik, minimal tiga bulan sekali.
- 10) Pemeliharaan ketersediaan pasokan air untuk peralatan AC dan pemadam kebakaran. Pemeriksaan sistem peringatan (alarm) harus diperiksa secara rutin.
- 11) Penyediaan jalur telekomunikasi ganda dari sisi *routing* untuk mengurangi risiko kegagalan komunikasi apabila salah satu jalur telekomunikasi yang ada terputus.

c. Pengamanan Pengkabelan

- 1) Kabel listrik dan Jaringan komunikasi harus

terlindungi dan tidak ditempatkan di area publik sehingga tidak mengalami kerusakan akibat ketidaksengajaan oleh personel maupun gangguan binatang.

- 2) Penggunaan penanda kabel di ruang server Jaringan guna mempermudah penanganan apabila terjadi masalah dan menghindari kesalahan. Penandaan kabel harus didokumentasikan dengan baik.
- 3) Pengamanan pengkabelan perlu mempertimbangkan beberapa hal berikut:
 - a) Pemasangan kabel listrik dan telekomunikasi yang digunakan untuk fasilitas pemrosesan informasi dilakukan sedemikian rupa sehingga dapat melindungi kabel dengan baik.
 - b) Pemasangan kabel listrik dan kabel komunikasi harus dilakukan secara terpisah.
 - c) Pemasangan perlindungan tambahan untuk sistem kritikal atau sensitif, di antaranya:
 - (1) Penggunaan pelindung kabel (*armoured conduit*) dan kotak atau ruangan terkunci untuk melindungi kabel terutama pada titik terminasi atau pemeriksaan.
 - (2) Penggunaan *routing* maupun media transmisi alternatif.
 - (3) Penggunaan pelindung kabel *fiber optic*.
 - (4) Penggunaan pelindung elektromagnetik.
 - (5) Pemeriksaan teknis secara fisik untuk memastikan tidak ada peralatan yang seharusnya tidak terhubung ke sistem komunikasi.
 - (6) Pengendalian Akses ke ruangan kabel dan *patch panel*.

d. Pemeliharaan Peralatan

- 1) Peralatan sistem informasi seperti perangkat keras dan Jaringan komunikasi, serta sarana pendukung harus dipelihara untuk menjamin ketersediaan dan integritas dari peralatan tersebut secara terus menerus.
- 2) Pemeliharaan peralatan dalam sistem informasi ANRI,

paling sedikit:

- a) Melakukan pemeliharaan peralatan secara rutin sesuai spesifikasi dan rekomendasi vendor.
- b) Aktivitas pemeliharaan dilakukan oleh personel yang memiliki kompetensi dan mendapat izin dari pihak yang mengelola perangkat.
- c) Setiap indikasi kerusakan yang terjadi serta perbaikan yang bersifat korektif dan preventif harus didokumentasikan dengan baik.
- d) Setiap pemeliharaan perlu mempertimbangkan informasi yang terdapat di dalam peralatan tersebut.

e. Pemindahan Peralatan Milik ANRI

- 1) Peralatan, informasi, maupun perangkat lunak milik ANRI atau milik pihak eksternal yang diserahkan pengelolaannya kepada ANRI tidak boleh dibawa keluar wilayah ANRI tanpa izin dari Pejabat terkait di ANRI.
- 2) Proses kendali keamanan saat pemindahan peralatan paling sedikit:
 - a) Hanya pihak mendapatkan otorisasi secara resmi yang bisa membawa aset hanya keluar area ANRI.
 - b) Setiap pemindahan aset keluar area ANRI Aset harus didokumentasikan.
 - c) Dilakukan pemeriksaan terhadap personel yang keluar dari area ANRI dengan membawa aset ANRI.

f. Pengamanan Peralatan di luar Wilayah ANRI

- 1) Penggunaan peralatan pengolahan informasi di luar wilayah ANRI mempertimbangkan kebutuhan penggunaannya.
- 2) Aset teknologi informasi yang bersifat portabel seperti *notebook* yang dibawa ke luar area kantor tidak boleh ditinggalkan di area publik tanpa pengamanan yang memadai dengan kabel pengunci serta *password*.
- 3) Pengamanan harus dilakukan pada semua aset yang terletak diluar area ANRI (*off premises*). Pengamanan ini perlu mempertimbangkan risiko yang muncul dari penggunaan peralatan dan pekerjaan di luar area

ANRI.

- 4) Penggunaan peralatan pengolahan informasi di luar area ANRI harus mendapatkan izin dari pihak pengelola/pemilik peralatan.
- 5) Pengamanan penggunaan aset di luar ANRI sekurang-kurangnya dilakukan dengan mematuhi ketentuan:
 - a) Informasi dan peralatan pengolahan informasi tidak boleh ditinggal di area umum tanpa pengawasan.
 - b) Instruksi dari vendor pembuat peralatan pengolahan informasi mengenai penggunaan peralatan tersebut harus dipatuhi.
 - c) Pengendalian keamanan bagi peralatan yang digunakan untuk bekerja dari rumah harus melalui proses penilaian risiko untuk menentukan metode kendali keamanan yang tepat.
 - d) Digunakannya jasa asuransi untuk melindungi ANRI dari kerugian yang mungkin muncul dari penggunaan peralatan di luar area ANRI.
- g. Pemusnahan, Perbaikan atau Penggunaan Kembali Peralatan secara Aman
 - 1) Harus dipastikan bahwa pada peralatan pengolahan informasi yang akan diperbaiki atau digunakan kembali tidak memiliki informasi sensitif yang masih terkandung sebelum peralatan tersebut diperbaiki atau digunakan kembali.
 - 2) Bagi peralatan pengolahan informasi yang tidak akan dipergunakan lagi dan di dalamnya terdapat informasi sensitif, maka informasi yang terkandung di dalamnya harus dihapus secara permanen dan peralatan harus dimusnahkan secara fisik sehingga tidak dimungkinkan lagi untuk mengambil informasi yang terkandung dalam peralatan tersebut.
 - 3) Seluruh aset teknologi informasi dan komunikasi yang akan dimusnahkan atau digunakan kembali harus diperiksa dan dipastikan bahwa tidak lagi terdapat data sensitif yang tersimpan dalam perangkat sehingga tidak dimungkinkan lagi untuk mengambil informasi

yang terkandung di perangkat tersebut.

- 4) Prosedur terkait dengan *disposal* dan penggunaan kembali peralatan diatur dalam prosedur pengelolaan aset.
- h. Perlindungan untuk Perangkat yang Tidak dalam Pengawasan Pengguna.
 - 1) Pengguna harus memastikan aset yang sedang tidak digunakan terlindungi dengan baik dengan menghentikan (*terminate*) *session* aktif terhadap sistem setelah selesai digunakan.
 - 2) Pengguna sedapat mungkin melakukan *log off* pada komputer atau server setelah *session* selesai digunakan.
 - 3) Pengguna harus mengamankan komputer atau terminal yang digunakan dengan menggunakan *password*.
- i. *Clear Desk* dan *Clear Screen*
 - 1) Seluruh pegawai di lingkungan ANRI harus menerapkan *clear desk* dan *clear screen* terkait dengan keamanan informasi yang rahasia atau sensitif.
 - 2) Komputer atau terminal harus di *log-off*/*screen saver lock* apabila sedang tidak digunakan atau diawasi.
 - 3) Dokumen yang mengandung informasi sensitif dari mesin *printer* maupun *photocopy* harus segera dipindahkan.
 - 4) *Clear desk*, yaitu setiap pegawai harus membersihkan meja dari segala informasi yang berkaitan dengan pekerjaan pada akhir jam kerja.
 - 5) *Clear screen*, yaitu setiap pegawai harus mengunci layar komputer ketika meninggalkan meja kerja dan melakukan *log off* bila meninggalkan meja kerja untuk jangka waktu lebih dari 5 (lima) menit.
 - 6) Seluruh pengguna bertanggung jawab untuk menerapkan *clear desk* dan *clear screen*.
- j. Penanggung Jawab Pengamanan Perangkat
Penanggung jawab pengamanan perangkat adalah masing- masing unit kerja yang menggunakan perangkat teknologi informasi dan komunikasi ANRI.

3. Keamanan Operasional

Prosedur pengelolaan tanggung jawab dan operasional, meliputi:

a. Prosedur Operasional yang Terdokumentasi

- 1) Setiap sistem yang dioperasikan di lingkungan ANRI harus dilengkapi dengan prosedur dan petunjuk pengoperasian, seperti *run book* atau *manual book*, dan dipelihara untuk menjaga ketersediaannya bagi seluruh pengguna sistem informasi yang membutuhkannya.
- 2) Prosedur operasional keamanan informasi harus sesuai dengan peraturan perundangan tentang standar teknis dan prosedur keamanan informasi;
- 3) Prosedur operasional harus secara spesifik mendeskripsikan rincian pelaksanaan kegiatan yang mencakup:
 - a) Pengelolaan kapasitas.
 - b) Pengelolaan perubahan.
 - c) *Backup* dan *restore*.
 - d) Prosedur penanganan insiden/gangguan selama aktivitas pekerjaan berlangsung.
 - e) Pihak yang harus dihubungi untuk mendapatkan dukungan (*support*) apabila terjadi masalah atau kesulitan.
 - f) Proses *restart* dan *recovery* sistem.
- 4) Seluruh dokumentasi prosedur operasional harus ditangani sesuai klasifikasinya dan sesuai dengan proses pengelolaan dokumentasi ANRI.

b. Pemisahan Lingkungan Pengembangan, Pengujian, dan Operasional

- 1) Pemisahan fasilitas sistem pengembangan, pengujian dan operasional di ANRI guna mengurangi risiko akses atau perubahan tanpa izin/tidak disengaja pada sistem operasional.
- 2) Identifikasi dan pengendalian tingkat pemisahan antara lingkungan pengembangan, pengujian dan operasional guna menjamin pemisahan tetap terjaga
- 3) Proses pemisahan harus mempertimbangkan hal-hal berikut:
 - a) Perangkat lunak atau aplikasi yang digunakan di lingkungan pengembangan dan operasional harus dijalankan pada sistem atau perangkat keras yang

terpisah.

- b) *Compiler, editor, dan tools* pengembangan lain tidak diperbolehkan untuk diakses dari sistem operasional kecuali sangat dibutuhkan.
 - c) Apabila memungkinkan, lingkungan pengujian harus memiliki kesamaan, baik dari sisi konfigurasi maupun spesifikasi, dengan lingkungan operasional.
 - d) Pengguna harus menggunakan *profil* pengguna yang berbeda ketika menjalankan sistem pada lingkungan operasional dan pengujian.
 - e) Menu dalam aplikasi harus menampilkan keterangan yang jelas untuk meminimalkan kesalahan pengguna dalam membedakan lingkungan sistem yang ada.
 - f) Data-data yang bersifat sensitif tidak diperbolehkan disalin ke lingkungan pengujian tanpa pengamanan yang memadai.
- 4) Ketentuan pemisahan berlaku untuk setiap unit kerja yang mengembangkan aplikasi.

c. Penanggung Jawab Pengelolaan Tanggung Jawab dan Prosedur Operasional

Penanggung jawab pengelolaan tanggung jawab dan prosedur operasional mempunyai tugas melaksanakan penyusunan tata kelola dan infrastruktur teknologi informasi dan komunikasi.

4. Manajemen Perubahan

- a. Seluruh perubahan dalam infrastruktur teknologi informasi dan komunikasi dan sistem aplikasi harus dikelola dan dikendalikan untuk menghindari terjadinya kegagalan dalam sistem informasi.
- b. Pengendalian perubahan yang diterapkan pada infrastruktur dan sistem harus mengacu pada prosedur yang sekurang-kurangnya berisi:
 - 1) Aspek risiko yang muncul terhadap kebutuhan bisnis.
 - 2) Dokumentasi atas *log* perubahan sesuai urutan waktu perubahan.
 - 3) Perencanaan dan pengujian perubahan.
 - 4) Proses persetujuan formal untuk usulan perubahan
 - 5) Proses review dan pemantauan atas pelaksanaan perubahan.

- c. Seluruh sistem operasional dan aplikasi perangkat lunak harus dikelola dan dikendalikan melalui manajemen perubahan formal.
 - d. Perubahan digolongkan berdasarkan tingkat kepentingannya, yaitu:
 - 1) Perubahan normal merupakan perubahan yang telah direncanakan terlebih dahulu.
 - 2) Perubahan darurat merupakan perubahan dibutuhkan untuk memperbaiki permasalahan pada sistem teknologi informasi dan komunikasi untuk mengembalikan proses operasional dengan cepat dan harus mendapatkan persetujuan dari pengelola sistem teknologi informasi dan komunikasi yang berwenang.
 - e. Manajemen perubahan mencakup namun tidak terbatas pada:
 - 1) *Assessment* dari potensi dampak, termasuk dampak dari sisi keamanan yang mungkin muncul dari perubahan.
 - 2) Prosedur persetujuan secara formal untuk setiap perubahan.
 - 3) Proses komunikasi seluruh rincian perubahan antar personel yang relevan.
 - 4) Prosedur *fall-back*, mencakup tanggung jawab dan prosedur untuk membatalkan dan pemulihan dari perubahan yang gagal dan kejadian yang tidak terduga sebelumnya.
 - f. Setiap perubahan harus melalui persetujuan terlebih dahulu sebelum dilaksanakan.
 - g. Setiap perubahan harus didokumentasikan.
5. Manajemen Kapasitas
- a. Setiap penanggung jawab sistem di ANRI harus menerapkan manajemen kapasitas untuk setiap pengembangan infrastruktur dan sistem aplikasi baru maupun yang sedang berjalan.
 - b. Manajemen kapasitas harus mempertimbangkan proyeksi kebutuhan operasional dan infrastruktur untuk kebutuhan layanan yang akan datang dan sistem informasi ANRI.
 - c. Proyek kebutuhan harus mempertimbangkan kondisi sistem informasi ANRI saat ini serta kecenderungan perkembangan sistem selama ini.
 - d. Pengukuran kapasitas terhadap aplikasi dan infrastruktur

dilakukan secara periodik.

- e. Pemantauan dan tuning atas penggunaan seluruh sumber daya pengolahan informasi dalam sistem informasi ANRI untuk memastikan ketersediaan dan kecukupan kapasitas.
- f. Semua aktivitas atau proses dalam sistem informasi baik yang sedang berjalan maupun yang akan dijalankan harus menyertakan identifikasi kebutuhan kapasitas sistem, antara lain kapasitas memori atau *storage* dalam *server*, utilisasi *central processing unit*, atau utilisasi *backbone* jaringan WAN.
- g. Perhatian lebih dalam hal manajemen kapasitas diterapkan pada sistem atau perangkat pengolahan informasi yang memiliki biaya tinggi secara finansial, waktu maupun penggunaan sumber daya manusia.
- h. Proses manajemen kapasitas perlu mempertimbangkan ketergantungan atau *bottleneck* terkait sumber daya manusia yang dapat menimbulkan ancaman terhadap aspek kerahasiaan, integritas maupun ketersediaan informasi dan sistem informasi ANRI.

6. Penggunaan Perangkat *Mobile*

Pengelolaan penggunaan perangkat *mobile* mencakup:

- a. Pengguna fasilitas *notebook* harus memperhatikan keamanan data yang disimpan dalam perangkat pada saat digunakan di luar area ANRI.
- b. Fasilitas *notebook* yang sedang digunakan di luar area ANRI harus dipastikan keamanannya secara fisik untuk mencegah terjadinya pencurian/kehilangan perangkat.
- c. Penggunaan perangkat *mobile* seperti *notebook* dan *smartphone* yang menyimpan informasi milik ANRI ataupun milik pihak eksternal yang telah diserahkan pengelolaannya kepada ANRI dilakukan dengan menerapkan kontrol keamanan yang baik untuk menangani risiko terhadap kerahasiaan, integritas dan ketersediaan informasi.
- d. Perlindungan atas perangkat *mobile* mencakup namun tidak terbatas pada perlindungan secara fisik, pengendalian akses ke peralatan perangkat *mobile*, kriptografi, *backup* dan perlindungan terhadap *malware* dan *virus*.
- e. Panduan, pelatihan dan program peningkatan kesadaran dilakukan secara teratur untuk memastikan pemahaman

setiap pegawai pengguna fasilitas perangkat *mobile* tentang risiko yang ada serta prosedur pengendaliannya.

7. Pengendalian Terhadap *Malware*

Pengguna sistem informasi di ANRI perlu memahami bahaya *malware* dan mengetahui bagaimana mencegah serta menanganinya.

Pengendalian terhadap *malware*, mencakup:

- a. Kendali terhadap *malware* dapat dilakukan melalui pendeteksian dan pencegahan serangan *malware* dan pemulihan setelah terjadi serangan *malware*.
- b. Pegawai di lingkungan ANRI harus melindungi sistem informasi dari serangan *malware* dengan tidak meng-*install* perangkat lunak ilegal, dan/atau *unwanted program*.
- c. Setiap perangkat seperti PC dan *notebook*, dan *server* harus menggunakan antivirus untuk mencegah bahaya *malware* (virus, *worm*, *trojan*).
- d. Setiap pegawai ANRI harus memastikan bahwa setiap *file* elektronik yang berasal dari media penyimpanan atau jaringan, termasuk *e-mail* dan internet, tidak mengandung virus dengan melakukan *scanning* terhadap *file* atau program tersebut sebelum mengakses atau menggunakan.
- e. *Update* dan *scanning* rutin harus dilakukan secara otomatis untuk mendeteksi virus pada komputer dan media penyimpanan. Proses pendeteksian mencakup:
 - 1) Data dalam media penyimpanan elektronik maupun optik dan data yang diperoleh melalui jaringan komunikasi sebelum digunakan.
 - 2) *Attachment e-mail*, perlu dilakukan pada beberapa titik dalam sistem informasi seperti *e-mail server*, pada perangkat jaringan dan komputer pengguna.
- f. Pemeliharaan secara terus menerus atas kesadaran (*awareness*) pengguna sistem informasi terhadap bahaya serangan *malware*.
- g. Perlindungan sistem informasi dari serangan *malware* dapat dilakukan oleh ANRI melalui kombinasi dari:
 - 1) Penggunaan perangkat lunak untuk mendeteksi dan memperbaiki kerusakan yang disebabkan oleh *malware*.
 - 2) Pelaksanaan program peningkatan kesadaran pengguna.
 - 3) Pengendalian akses ke sistem informasi dan pengelolaan perubahan.

h. Perlindungan sistem informasi dari serangan *malware* dilakukan dengan mengimplementasikan beberapa hal berikut:

- 1) ANRI hanya menggunakan perangkat lunak yang diizinkan secara legal/formal.
- 2) Antivirus yang terpasang harus dikonfigurasi untuk beroperasi secara terus-menerus pada sistem teknologi informasi dan komunikasi. Pengguna dilarang mengubah konfigurasi perangkat lunak antivirus yang terpasang.
- 3) Peninjauan berkala harus dilakukan terhadap *software* dan data yang digunakan untuk mendukung proses bisnis guna memastikan tidak terdapat data atau perangkat lunak yang tidak diizinkan dalam sistem informasi ANRI.
- 4) Apabila tidak memungkinkan untuk dilakukan *updating* secara otomatis, maka harus disediakan prosedur untuk melakukan proses *updating* secara manual.
- 5) Panduan tindakan yang harus dilakukan pada perangkat teknologi dan informasi untuk menangani infeksi *malware* harus didefinisikan, didokumentasikan dan diinformasikan kepada pengguna. Panduan tersebut harus mencakup tindakan-tindakan sebagai berikut:
 - (a) Pengisolasian *flash disk* dan media eksternal lainnya yang diduga terinfeksi virus.
 - (b) Pembersihan sesegera mungkin untuk komputer, *server*, *workstation* yang diduga terinfeksi virus.
 - (c) Melaporkan semua kejadian yang berkaitan dengan virus kepada petugas yang berwenang dan dicatat dalam *log insiden pengamanan (security incident)*.
- 6) Penggunaan perangkat lunak untuk pengendalian *malware* perlu dilengkapi dengan pengaktifan fungsi *update* secara otomatis.

i. Penanggung Jawab Pengendalian Terhadap *Malware*

Penanggung jawab pengendalian terhadap *malware* adalah unit kerja yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi.

8. Pengelolaan *Backup*

Pengelolaan *backup* mencakup:

- a. Informasi yang bersifat rahasia atau kritis (memiliki tingkat

integritas dan ketersediaan tinggi) harus memiliki *backup* sebagai pengganti dalam hal data/informasi utama tidak dapat dibaca, rusak, atau mengalami gangguan lainnya.

- b. Frekuensi dan tingkat *backup* (penuh atau parsial) disesuaikan dengan kebutuhan kritikalitas bisnis,
- c. Hasil *backup* harus disimpan pada tempat yang aman dan diusahakan ditempatkan di luar lokasi utama serta diberikan perlindungan secara fisik dan lingkungan yang memadai.
- d. Media *backup* harus diuji secara berkala melalui uji *restore* untuk memastikan media tersebut dapat berfungsi dengan baik pada saat dibutuhkan.
- e. Masa retensi dari *backup* informasi tergantung dari tingkat kritikalitas informasi dan sistem yang dioperasikan di ANRI.
- f. Informasi yang dimiliki ANRI harus secara rutin di-*backup* sesuai dengan kebijakan dan strategi *backup* formal ANRI.
- g. Fasilitas *backup* yang memadai harus disediakan untuk memastikan bahwa proses pemulihan (*recovery*) dapat dilakukan untuk seluruh informasi dan perangkat lunak yang dibutuhkan apabila terjadi gangguan atau bencana.
- h. Proses *backup* informasi mempertimbangkan hal - hal sebagai berikut:
 - 1) Informasi yang perlu di-*backup* harus ditentukan.
 - 2) Daftar informasi yang telah di-*backup* harus didokumentasikan dalam sebuah *record* yang terpelihara.
 - 3) Prosedur *restore* harus diuji secara berkala untuk memastikan *restore* dapat dilakukan secara efektif dan selesai dilakukan dalam jangka waktu yang telah ditentukan.
 - 4) *Backup* informasi yang bersifat sensitif dilengkapi pengamanan *enkripsi*.
- i. Penanggung Jawab Pengelolaan *Backup*
Penanggung jawab pengelolaan *backup* adalah unit kerja yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi.

9. Pengelolaan *Logging* dan Pemantauan

Pengelolaan *logging* dan pemantauan mencakup:

- a. Pengelolaan *Event Logging*

- 1) Perekaman dan penyimpanan *log* audit pada sistem untuk memantau aktivitas pengguna dalam jangka waktu yang ditentukan.
 - 2) *Log* audit yang perlu disimpan mencakup aspek berikut:
 - (a) *User id*, tanggal dan waktu serta rinci dari kejadian penting (*key events*) dalam sistem seperti *log-on* dan *log-off*.
 - (b) *Records* untuk percobaan akses baik yang berhasil maupun gagal.
 - (c) Ide perubahan pada konfigurasi sistem.
 - (d) Penggunaan hak akses khusus.
 - (e) Data yang diakses dan jenis aksesnya.
 - (f) Alamat dan protokol jaringan.
 - (g) Peringatan alarm yang dibuat oleh sistem pengendalian akses.
 - (h) Pengaktifan dan penonaktifan sistem pengamanan seperti sistem antivirus atau *intrusion detection system* dari terminal atau komputer.
 - 3) Pembuatan dan pemeliharaan *event log* yang digunakan untuk merekam aktivitas pengguna, pengecualian (*exception*), kegagalan (*fault*), dan kejadian keamanan informasi yang ditetapkan berdasarkan kategori dan tingkat vitalitas Sistem Elektronik, tingkat risiko, kebutuhan pemantauan, investigasi, audit, forensik, kapasitas penyimpanan, dan ketentuan peraturan perundang-undangan.
 - 4) Penyesuaian pengamanan *log audit yang* berisi informasi yang bersifat sensitif.
- b. Penerapan Security Information and Event Management
- Dalam rangka meningkatkan kemampuan deteksi, korelasi, analisis, dan respons terhadap kejadian keamanan informasi, ANRI menerapkan dan mengelola Security Information and Event Management (SIEM) secara terpusat sesuai dengan tingkat risiko, kritikalitas aset, dan kebutuhan layanan.
- Penerapan SIEM sebagaimana dimaksud dilakukan untuk mengumpulkan, menyimpan, mengorelasikan, menganalisis, dan memantau log aktivitas keamanan informasi yang berasal dari sumber-sumber log yang relevan, paling sedikit meliputi:

1. perangkat jaringan;
2. perangkat keamanan jaringan;
3. server dan sistem operasi;
4. aplikasi dan basis data;
5. endpoint;
6. aktivitas pengguna;
7. aktivitas administrator dan operator sistem; dan
8. sistem pendukung layanan teknologi informasi dan komunikasi lainnya.

Pengelolaan SIEM dilakukan dengan memperhatikan sinkronisasi waktu, integritas log, retensi log, perlindungan terhadap perubahan dan penghapusan log tanpa izin, pengaturan hak akses terhadap SIEM, serta pemantauan atas peringatan keamanan yang dihasilkan.

Hasil korelasi dan analisis SIEM digunakan sebagai dasar untuk deteksi dini, validasi kejadian keamanan informasi, eskalasi insiden, investigasi, pelaporan, peningkatan kontrol keamanan, dan perbaikan berkelanjutan.

Penanggung jawab penerapan dan pengelolaan SIEM adalah unit kerja yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi, dengan melibatkan unit kerja terkait sesuai dengan kebutuhan penanganan kejadian dan insiden keamanan informasi.

c. Perlindungan Terhadap Informasi *Log*

- 1) Perlindungan *log* sistem dari modifikasi dan akses tanpa izin yaitu pembatasan terhadap perubahan atau penghapusan terhadap *log files*.
- 2) Administrator sistem harus memastikan kapasitas penyimpanan *log files* guna menghindari kegagalan dalam pencatatan kejadian atau *overwriting* kejadian yang lama.
- 3) Penyimpanan *audit log* harus mempertimbangkan masa retensi yang telah ditentukan dan kebutuhan untuk pengumpulan bukti audit.

d. Pengelolaan *Log* bagi Administrator dan Operator Sistem

- 1) Perekaman dan peninjauan secara berkala atas aktivitas administrator dan operator sistem informasi di dalam *log* yang mencakup:
- 2) Waktu kejadian baik yang sukses maupun gagal.

- 3) Hak Akses dan identitas dari administrator atau operator.
 - 4) Informasi mengenai kejadian atau kegagalan yang terjadi.
 - 5) Proses yang sedang berjalan saat kejadian terjadi.
 - 6) Peninjauan *log* bagi administrator dan operator secara rutin.
- e. Sinkronisasi Waktu
- 1) *Clock* seluruh sistem pengolahan informasi ANRI atau sebuah domain jaringan informasi harus di sinkronisasi.
 - 2) Penerapan sinkronisasi waktu sesuai standar waktu yang ditetapkan pada sistem pengolahan informasi seperti server yang memiliki fungsi *real time clock*.
 - 3) Administrator server harus memastikan waktu pada setiap sistem kritikal server harus disinkronisasi dengan standar waktu yang berlaku secara internasional dan melakukan pemantauan dan koreksi apabila terdapat deviasi.
 - 4) Penerapan sinkronisasi *clock* guna menjamin akurasi *log audit*.
- f. Penanggung Jawab Pengelolaan *Logging* dan Pemantauan
- Penanggung jawab pengelolaan *logging* dan pemantauan adalah unit kerja yang melaksanakan tugas atau fungsi layanan di bidang teknologi informasi dan komunikasi.

10. Keamanan Komunikasi dan Sistem Informasi

a. Pengelolaan Keamanan Jaringan

Pengelolaan keamanan jaringan ANRI harus mempertimbangkan:

- 1) Pemeliharaan diagram topologi jaringan yang mencakup komponen jaringan pada *data center*.
- 2) Pemeliharaan sistem yang terhubung dengan jaringan komunikasi.
- 3) Pelaporan seluruh permasalahan jaringan komunikasi kepada pejabat yang berwenang dan penanganannya harus sesuai dengan proses penanganan masalah.
- 4) Penerapan manajemen perubahan dan otorisasi untuk setiap perubahan terhadap jaringan komunikasi.
- 5) Penggunaan fasilitas koneksi internet hanya untuk tujuan keperluan layanan ANRI.
- 6) Perencanaan kapasitas jaringan komunikasi dan analisis kinerja harus dilakukan secara berkala.
- 7) Pemantauan infrastruktur jaringan komunikasi.

b. Pengendalian Jaringan

- 1) Akses jaringan eksternal ke pusat data anri dapat dilakukan dengan sangat terbatas dan dengan menggunakan perangkat komputer yang terpisah dari jaringan ANRI.
- 2) Dalam penggunaan *shared network*, hak akses pengguna untuk mengakses jaringan ANRI yang dikelola oleh ANRI harus dibatasi sesuai dengan pengendalian akses.
- 3) Jaringan perlu dikelola dan dikendalikan untuk melindungi sistem informasi yang terdapat di dalamnya.
- 4) Dalam pengendalian jaringan, secara khusus hal berikut perlu dipertimbangkan:
 - (a) Apabila memungkinkan, personel yang bertanggung jawab untuk operasional jaringan dipisahkan dengan personel yang bertanggung jawab untuk operasional komputer dan server.
 - (b) Pengaksesan jaringan menggunakan perangkat akses *remote* hanya dimungkinkan jika dilakukan berdasarkan prosedur yang baku.
 - (c) Penerapan kontrol khusus untuk menjaga kerahasiaan dan integritas informasi yang dikirimkan melalui jaringan publik dan *wireless*.
 - (d) Pengelolaan jaringan (*network* manajemen) yang meliputi *logging*, *monitoring*, *incident response* dan *network traffic* manajemen dilakukan secara terkendali dan konsisten.
 - (e) Tersedianya jejak audit (*audit trail*), sekurang-kurangnya terhadap perubahan-perubahan pada *setting* parameter dan hak akses perangkat jaringan komunikasi dan juga penggunaan atas hak akses tersebut.
 - (f) Akses ke jaringan ANRI harus dibatasi dan setiap akses perlu diotentikasi sebelum akses ke jaringan diberikan.
 - (g) Kepastian penggunaan perangkat pengamanan jaringan komunikasi, yang mencakup namun tidak terbatas pada *firewall*, *Intrusion Detection System* (IDS), dan *Intrusion Prevention System* (IPS).
 - (h) Pengujian terhadap keamanan jaringan komunikasi,

misalnya dengan *penetration testing* harus dilakukan secara berkala

- (i) Pengukuran kinerja dan perencanaan kapasitas jaringan (*performance and capacity planning*) dilakukan secara berkala.

c. Keamanan Layanan Jaringan

- 1) Layanan jaringan mencakup seluruh layanan sistem informasi ANRI yang menggunakan jaringan komunikasi dalam operasionalnya, seperti *e-mail*, internet dan layanan aplikasi ANRI antar satker.
- 2) Layanan jaringan meliputi penyediaan koneksi, layanan jaringan *private* dan *value added network* serta solusi pengembangan dan/atau pengelolaan keamanan jaringan seperti sistem *firewall* dan *intrusion detection system*.
- 3) Teknologi pengamanan layanan jaringan dapat berupa otentifikasi, enkripsi dan pengendalian koneksi jaringan.
- 4) Fitur keamanan, tingkat layanan dan kebutuhan terhadap layanan Jaringan yang diidentifikasi dalam operasional sistem di ANRI harus dimonitor dan dievaluasi secara berkala.
- 5) Seluruh perjanjian layanan jaringan, tanpa memandang apakah layanan jaringan diberikan oleh pihak internal maupun eksternal harus mengidentifikasi fungsi keamanan, tingkat layanan dan *requirement* dari ANRI.

d. Pemisahan dalam Jaringan

- 1) Jaringan yang disediakan harus dipisahkan antara kelompok layanan informasi, user, dan sistem informasi.
- 2) Pemisahan pada jaringan internal dilaksanakan oleh ANRI berdasarkan kebutuhan operasional dan sensitivitas sistem.
- 3) Pemisahan diimplementasikan dengan membagi jaringan menjadi domain jaringan yang terpisah, baik secara fisik.
- 4) Pemisahan yang pertama kali harus dilakukan adalah memisahkan antara domain jaringan internal dengan jaringan eksternal ANRI.
- 5) Pemisahan harus didasari oleh penilaian risiko yang menyeluruh untuk menganalisis kebutuhan keamanan informasi dari masing-masing domain yang ada dan untuk

pengaturan akses dan arus informasi antar domain jaringan.

- 6) Pemisahan jaringan yang dilakukan untuk memisahkan jaringan *wireless* ANRI harus dilengkapi dengan kontrol keamanan seperti metode kriptografi serta otentifikasi.
- 7) Pemisahan dalam Jaringan dapat diimplementasikan dengan antara lain:
 - (a) Pemasangan *secure gateways* seperti *firewall* antara domain jaringan untuk mengatur akses dan arus informasi dengan cara melakukan *traffic filtering* antar domain jaringan.
 - (b) Mengimplementasikan virtual LAN untuk setiap domain atau group pengguna sistem informasi ANRI.

e. Penanggung Jawab Pengelolaan Keamanan Jaringan

Penanggung jawab pengelolaan keamanan jaringan adalah unit kerja yang melakukan tugas atau fungsi layanan di bidang teknologi informasi dan komunikasi.

11. Pengelolaan *Technical Vulnerability*

Penerapan pengelolaan *technical vulnerability* secara efektif, sistematis mencakup:

a. Pengendalian Kelemahan teknis (*Technical Vulnerability*)

- 1) Pengujian terhadap setiap perubahan sistem operasi pada server sistem informasi ANRI harus dilakukan agar tidak mengganggu keberlangsungan operasional yang mencakup kepastian keandalan sistem informasi.
- 2) Informasi mengenai kelemahan dari sistem informasi ANRI harus diperoleh tepat waktu. Informasi tersebut tidak boleh terungkap ke pihak lain dan dikendalikan melalui proses *risk assessment*.
- 3) Pelaksanaan inventarisasi aset informasi yang lengkap dan terkini mencakup vendor perangkat lunak, versi perangkat lunak, status dari penggunaan serta pegawai yang bertanggung jawab.
- 4) Pengelolaan potensi kelemahan teknis dilaksanakan sekurang- kurangnya dengan mekanisme berikut:
 - (a) Identifikasi sumber daya yang dibutuhkan untuk mengidentifikasi kelemahan teknis perangkat pengolah informasi dan untuk menjaga *awareness*

mengenai kelemahan tersebut.

- (b) Penetapan jangka waktu penanganan kelemahan teknis maupun potensi risiko yang diidentifikasi, ditetapkan berdasarkan tingkat keparahan, kemungkinan eksploitasi, ketersediaan exploit, paparan aset, kategori dan tingkat vitalitas Sistem Elektronik, serta dampak terhadap layanan. Pengecualian wajib disertai penerimaan risiko dan kontrol kompensasi.
- (c) Setelah kelemahan teknis diidentifikasi, perlu diambil tindakan berdasarkan identifikasi risiko yang timbul.
- (d) Pelaksanaan perubahan untuk mengatasi kelemahan berdasarkan proses pengelolaan perubahan dan penanganan insiden keamanan informasi.
- (e) Pelaksanaan analisis risiko atas patching yang ditujukan untuk mengatasi kelemahan teknis guna membandingkan risiko antara kelemahan teknis yang ada sebelum dan sesudah proses *patching*.
- (f) Setiap *patch* perlu diuji dan dievaluasi sebelum diinstall untuk memastikan tidak ada efek negatif dari instalasi tersebut. Apabila pengujian tidak memungkinkan untuk dilakukan maka evaluasi dapat dilakukan berdasarkan pengalaman dari pengguna lain dari sistem yang sama.
- (g) Apabila *patch* untuk mengatasi kelemahan teknis tersebut tidak ditemukan maka dapat dipertimbangkan pengendalian sebagai berikut:
 - (1) Mematikan layanan atau perangkat sistem informasi yang memiliki dan/atau terkait dengan kelemahan teknis tersebut.
 - (2) Mengubah atau menambah kontrol akses, seperti *access control list* pada *firewall*.
 - (3) Meningkatkan monitoring sistem untuk mendeteksi atau mencegah adanya eksploitasi kelemahan teknis.
 - (4) Meningkatkan kesadaran akan adanya kelemahan teknis.
 - (5) Memelihara *audit log* untuk seluruh prosedur

yang terkait dengan kelemahan teknis.

(6) Secara reguler melakukan pengawasan dan evaluasi proses pengelolaan kelemahan teknis untuk menjamin efektivitas dan efisiensi.

(7) Menetapkan sebagai prioritas pertama untuk sistem dengan risiko tinggi.

b. Pembatasan Instalasi Perangkat Lunak

1) Perubahan atau modifikasi perangkat lunak harus dikendalikan untuk memastikan keberlangsungan layanan jaringan.

2) Perangkat lunak yang digunakan harus berlisensi resmi atau bersifat bebas lisensi (*freeware*)/*open source* dan sesuai dengan aturan keamanan informasi yang ada di ANRI.

3) Pengguna dilarang melakukan instalasi perangkat lunak tanpa otorisasi dari pihak yang berwenang.

4) Instalasi perangkat lunak harus dilakukan oleh administrator sistem terkait.

c. Penanggung Jawab Pengelolaan *Technical Vulnerability*

Penanggung jawab pengelolaan *technical vulnerability* adalah unit kerja yang melaksanakan tugas atau fungsi layanan di bidang teknologi informasi dan komunikasi.

12. Pengelolaan Kejadian Insiden dan Keberlangsungan Operasional

a. Pengelolaan Insiden Keamanan Informasi

Pengelolaan insiden keamanan informasi mencakup:

1) Tanggung jawab dan prosedur penanganan insiden keamanan informasi.

a) ANRI bertanggung jawab untuk memastikan bahwa pihak yang melaksanakan penanganan insiden informasi pada pusat data mempunyai kewenangan dalam mengoordinasikan tindak lanjut insiden secara cepat dan efektif.

b) Prosedur penanganan insiden keamanan informasi harus mempertimbangkan aspek-aspek berikut:

(1) Prosedur harus mencakup penanganan berbagai tipe insiden keamanan informasi, yang meliputi namun tidak terbatas pada:

(a) *Malware virus, worm, trojan horse*, atau jenis

program jahat lainnya yang berhasil menginfeksi suatu *host*.

- (b) *Denial of service* suatu serangan yang mengakibatkan penolakan atau gangguan atas penggunaan sistem, jaringan, atau aplikasi.
 - (c) *Component* suatu insiden yang merupakan gabungan dari beberapa jenis insiden.
 - (d) Kesalahan yang diakibatkan oleh data yang tidak lengkap atau tidak akurat.
 - (e) Kebocoran informasi yang menyebabkan hilangnya aspek kerahasiaan dan integritas informasi.
 - (f) Penyalahgunaan sistem informasi.
 - (g) Ketidakpatuhan terhadap kebijakan dan prosedur yang berlaku.
 - (h) Hilangnya layanan, peralatan atau fasilitas pengolahan informasi.
- (2) Kerusakan pada perangkat lunak maupun perangkat keras. Selain mencakup rencana penanggulangan, prosedur juga harus mencakup:
- (a) Analisis dan identifikasi penyebab insiden.
 - (b) Panduan melokalisir insiden sehingga tidak menyebar (*containment*).
 - (c) Perencanaan dan implementasi tindakan korektif, bila diperlukan, untuk mencegah terulangnya insiden tersebut.
 - (d) Panduan komunikasi dengan pihak-pihak yang terkait dalam pemulihan dari insiden tersebut.
 - (e) Pelaporan tindakan yang dilakukan kepada pihak yang berwenang.
- (3) Pengumpulan bukti atau *audit trail* beserta pengamanannya untuk keperluan:
- (a) Analisis permasalahan secara internal.
 - (b) Penggunaannya sebagai bukti forensik untuk mencari potensi pelanggaran kontrak, regulasi atau digunakan sebagai bukti dalam proses hukum.

- (c) Material pendukung negosiasi kompensasi dari pihak ketiga.
- (4) Pengendalian tindakan pemulihan dari pelanggaran keamanan serta koreksi kegagalan sistem guna menjamin:
 - (a) Hanya pegawai yang berwenang yang dapat mengakses data dan sistem yang berjalan.
 - (b) Seluruh tindakan darurat terdokumentasi secara rinci.
 - (c) Pelaporan tindakan darurat kepada pejabat yang berwenang.
 - (d) Peninjauannya tindakan darurat.
- (5) Personel yang memiliki tugas dan tanggung jawab pengelolaan insiden keamanan informasi harus memahami proses beserta prioritas penanganan insiden keamanan informasi.
- (6) Keterlibatan unit lain yang terkait dalam melaksanakan penanganan insiden jika diperlukan.
- (7) Apabila diperlukan dan memungkinkan, koordinasi dengan Pihak Ketiga dapat dilakukan untuk mengoordinasikan tindakan serta membagi informasi mengenai insiden keamanan informasi.

b. Pelaporan Insiden dalam Sistem Keamanan Informasi

- 1) Seluruh pegawai ANRI wajib melaporkan insiden keamanan informasi yang teridentifikasi melalui mekanisme pelaporan insiden di ANRI selambat-lambatnya dalam waktu 3x24 jam sejak insiden diketahui".
- 2) Panduan pelaporan dan penanganan insiden keamanan informasi ditetapkan dalam bentuk prosedur formal pelaporan insiden keamanan informasi serta prosedur penanganan dan eskalasi yang menjabarkan tindakan yang harus diambil pada saat penerimaan laporan.
- 3) Pelaporan ditujukan kepada *point of contact*. Perlu dipastikan juga bahwa *point of contact* ini diketahui oleh pengguna sistem informasi ANRI, selalu tersedia dan dapat memberikan tanggapan secara tepat dan cepat untuk

setiap laporan.

- 4) Seluruh pengguna sistem informasi, baik pegawai, kontraktor atau Pihak Ketiga harus memahami tanggung jawabnya untuk secepat mungkin melaporkan kejadian keamanan informasi.
- 5) Pengguna sistem informasi harus memahami prosedur pelaporan kejadian dalam sistem informasi ANRI beserta *point of contact* untuk melaporkan kejadian tersebut.
- 6) Prosedur pelaporan harus mencakup antara lain:
 - (a) Proses *feedback* yang memastikan pemberitahuan kepada pelapor, setelah laporan selesai ditindaklanjuti.
 - (b) Formulir/dokumentasi pelaporan kejadian keamanan informasi untuk mendukung tindakan yang diambil berdasarkan laporan yang ada serta untuk membantu pegawai pelapor dalam mengingat langkah-langkah yang perlu dilakukan apabila terjadi gangguan keamanan informasi.
 - (c) Tindakan yang harus diambil apabila terjadi gangguan dalam sistem keamanan Informasi Elektronik seperti:
 - (1) Mencatat dengan segera seluruh kejadian secara rinci seperti tipe kejadian atau *non compliance*, kerusakan yang terjadi atau pesan kesalahan pada sistem.
 - (2) Segera melaporkan kepada *point of contact* yang telah ditetapkan, dan tidak mengambil tindakan sendiri.
 - (d) Penerapan sanksi sesuai aturan formal yang ditetapkan harus dilaksanakan untuk menangani pegawai atau Pihak Ketiga yang melakukan pelanggaran keamanan informasi.
- 7) Daftar kejadian gangguan keamanan informasi mencakup namun tidak terbatas pada:
 - (a) Tidak efektifnya kontrol keamanan informasi.
 - (b) Kegagalan atau *overload* dari sistem informasi.
 - (c) Kesalahan manusia.
 - (d) *Non-compliance* dengan kebijakan dan prosedur.

- (e) Tembusnya pengamanan fisik dan lingkungan.
- (f) Pergantian sistem yang tidak terkendali.
- (g) Kegagalan fungsi perangkat lunak dan keras.
- (h) Pelanggaran hak akses.

c. Proses Pelaporan Kelemahan dalam Sistem Keamanan Informasi

- 1) Seluruh pegawai ANRI yang menggunakan sistem wajib melaporkan kelemahan dalam sistem dan jaringan secepat mungkin untuk mencegah terjadinya insiden keamanan informasi.
- 2) Seluruh pengguna sistem informasi ANRI, termasuk pegawai dan Pihak Ketiga, harus melaporkan kelemahan dalam sistem keamanan informasi ANRI sesegera mungkin melalui mekanisme yang telah ditetapkan untuk mencegah terjadinya insiden keamanan informasi.
- 3) Mekanisme pelaporan harus mudah diakses dan selalu tersedia.
- 4) Bagi pelapor dilarang untuk membuktikan sendiri dugaan kelemahan yang ditemukan, seperti dengan melakukan *penetration test* tanpa izin.

d. *Assessment* dan Keputusan Terhadap Kejadian Keamanan Informasi

- 1) Asesmen terhadap kejadian keamanan informasi harus dilakukan untuk menentukan klasifikasi apakah kejadian tersebut termasuk insiden keamanan informasi, atau kejadian kelemahan sistem.
- 2) Hasil asesmen dan keputusan seperti pada nomor 12 poin a digunakan sebagai pertimbangan untuk menentukan tindakan- tindakan yang bertujuan untuk meminimalkan risiko terhadap ketersediaan, integritas, atau kerahasiaan informasi serta mencegah insiden lebih lanjut.

e. Respons Terhadap Insiden Keamanan Informasi

- 1) Panduan respons terhadap insiden keamanan informasi ditetapkan dalam prosedur respons terhadap keamanan informasi.
- 2) Pihak yang terkait (pimpinan, pegawai, Pihak Ketiga) harus menanggapi laporan insiden keamanan informasi yang datang kepadanya.
- 3) Penanganan insiden harus memperhatikan hal-hal

sebagai berikut:

- (a) Pengumpulan bukti terkait dengan insiden keamanan informasi.
- (b) Proses eskalasi penanganan insiden.
- (c) Dokumentasi proses penanganan.
- (d) Komunikasi dengan pihak-pihak yang terkena dampak dan terkait dengan insiden.

f. Proses Pembelajaran dari Insiden Keamanan Informasi

- 1) Setiap insiden keamanan informasi yang terjadi harus dievaluasi terkait dampak dan biaya serta digunakan sebagai bahan masukan untuk proses peninjauan kebijakan keamanan informasi.
- 2) ANRI harus menetapkan mekanisme untuk menghitung dampak yang timbul dari insiden keamanan informasi
- 3) Informasi yang diperoleh dari evaluasi insiden keamanan informasi harus digunakan untuk mengidentifikasi insiden yang berulang atau yang berdampak besar.

g. Pengumpulan Bukti (*evidence*)

- 1) Bukti tindak lanjut penanganan insiden harus dikumpulkan, disimpan, dan ditunjukkan terkait dengan proses audit dan/atau *evidence trail* di kemudian hari.
- 2) Bukti dalam bentuk *softcopy* harus dijamin tersimpan dengan aman dan dapat selalu diakses jika dibutuhkan.
- 3) Panduan dan aturan dalam pengumpulan bukti sekurang-kurangnya mencakup:
 - (a) Kualitas dan kelengkapan bukti.
 - (b) Sistem informasi ANRI harus disesuaikan dengan standar atau peraturan sistem informasi untuk mengumpulkan dan menghasilkan bukti. misal dengan menerapkan *log* sistem atau *audit trail* agar dapat dipastikan bahwa bukti yang dikumpulkan dapat digunakan dalam proses peradilan.
 - (c) Kualitas dan kelengkapan kontrol yang digunakan untuk melindungi bukti selama proses pengumpulan bukti, termasuk penyimpanan dan pengolahan bukti, harus didukung dengan proses audit dan/atau *evidence trail* yang baik.

h. Penanggung Jawab Pengelolaan Insiden Keamanan Informasi dan Perbaikan Terhadap Sistem

Penanggung jawab pengelolaan insiden keamanan informasi dan perbaikan terhadap sistem adalah unit kerja yang melaksanakan tugas atau fungsi layanan di bidang teknologi informasi dan komunikasi.

13. Manajemen Konfigurasi

- a. Inventarisasi aset teknologi dan informasi yang digunakan dalam infrastruktur mencakup perangkat keras, perangkat lunak, sistem operasi, aplikasi, beserta perangkat jaringan yang digunakan untuk membantu dalam pengelolaan konfigurasi dan pemantauan keamanan.
- b. Pengelolaan perubahan konfigurasi meliputi evaluasi perubahan yang diajukan, pengujian perubahan dan pemantauan dampak dari perubahan konfigurasi terhadap keamanan dan kinerja sistem.
- c. Penerapan prinsip hak akses berlaku untuk akses yang diperlukan sehingga mencegah penyalahgunaan akses.
- d. Audit terhadap *configuration item* dilakukan untuk memverifikasi kepatuhan terhadap standar konfigurasi dan kebijakan organisasi sekurangnyanya sekali dalam dua tahun.

14. *Web Filtering*

- a. ANRI perlu mengurangi risiko personelnnya mengakses situs web yang berisi informasi ilegal atau diketahui mengandung virus atau *phishing*.
- b. Pemblokiran IP dan *domain web* perlu dilakukan untuk mencegah akses kepada pengguna layanan jaringan. Penerapan *blacklist domain* dan IP web dapat dilakukan dalam perangkat jaringan.
- c. Pemblokiran penggunaan aplikasi yang digunakan untuk mengakses situs berbahaya dan ilegal.
- d. Pertimbangan blokir IP dan domain web dengan kriteria:
 - 1) Situs web yang memiliki fungsi pengunggahan informasi kecuali diizinkan untuk alasan bisnis yang sah;
 - 2) Situs web berbahaya yang diketahui atau dicurigai yang diperoleh dari aktivitas *threat intelligence* (situs web yang mendistribusikan *malware* atau konten *phishing*);
 - 3) Situs web berbagi konten ilegal.

15. Pengendalian *Redundancies*

Pengendalian Ketersediaan dari Fasilitas Pemrosesan Informasi ANRI mencakup:

- a. Pemasangan sistem *redundancy* yang mencukupi pada fasilitas pemrosesan jaringan untuk memenuhi kebutuhan layanan jaringan dan ketersediaan sistem.
- b. Apabila sistem *redundancy* tidak dapat dipenuhi, maka harus diimplementasikan proses alternatif untuk memastikan ketersediaan proses kegiatan dan operasional.
- c. Pengujian secara berkala harus dilakukan terhadap fasilitas pengolahan informasi dan sarana pendukungnya yang telah memenuhi aspek *redundancy* guna menjamin kesesuaian fungsinya.
- d. Penanggung jawab pengendalian *redundancies* adalah unit kerja yang melaksanakan tugas atau fungsi layanan di bidang teknologi informasi dan komunikasi.

C. Aplikasi

1. Pengelolaan Penyediaan Layanan (*Service Delivery*) Pengelolaan penyediaan layanan meliputi:

- a. Pemantauan dan Peninjauan Layanan dari Supplier
 - 1) Pemantauan terhadap layanan yang disediakan oleh pihak ketiga meliputi antara lain:
 - (a) Memantau tingkat layanan yang diberikan sesuai dengan perjanjian kerja.
 - (b) Mengkaji laporan yang disampaikan oleh pihak ketiga dengan melakukan pertemuan berkala yang dituangkan dalam risalah rapat atau laporan progress pelaksanaan pekerjaan pihak ketiga.
 - 2) Layanan, laporan dan *record* yang diberikan oleh pihak ketiga harus diawasi dan ditinjau secara rutin. Layanan, laporan dan *record* harus diaudit secara rutin.
 - 3) Pengawasan dan peninjauan kinerja pihak ketiga dilakukan untuk memastikan bahwa persyaratan dan ketentuan yang terkait dengan keamanan informasi dalam perjanjian kerja telah dijalankan dengan baik.
 - 4) Proses pengelolaan insiden maupun masalah keamanan informasi pada layanan pihak ketiga mencakup:

- (a) Pemberian informasi dan peninjauan laporan terkait dengan insiden keamanan informasi yang diberikan oleh pihak ketiga.
 - (b) Peninjauan *audit trail*, *security event*, permasalahan operasional, dan kegagalan dari pihak ketiga.
 - (c) Penyelesaian dan pengelolaan permasalahan yang telah teridentifikasi.
- 5) Bila diperlukan, dapat dilakukan audit terhadap pihak ketiga untuk memastikan kinerja dan pelayanan yang diberikan telah sesuai dengan perjanjian atau kontrak yang telah ditetapkan.
- b. Pengelolaan Perubahan Layanan dari Pihak Ketiga
- 1) Seluruh perubahan layanan yang diberikan oleh pihak ketiga, termasuk harus operasional dan pemeliharaan dikelola dengan mempertimbangkan sistem yang dijalankan oleh ANRI.
 - 2) Manajemen perubahan layanan pihak ketiga harus mempertimbangkan hal-hal berikut:
 - a) Perubahan yang diterapkan ANRI untuk mengimplementasikan:
 - (1) Peningkatan layanan ANRI.
 - (2) Pengembangan sistem dan aplikasi informasi baru.
 - (3) Modifikasi atau update kebijakan dan prosedur yang dimiliki ANRI.
 - (4) Kontrol baru untuk mengatasi insiden keamanan informasi dan untuk meningkatkan keamanan informasi ANRI.
 - b) Perubahan layanan pihak ketiga untuk mengimplementasikan:
 - (1) Perubahan dan peningkatan jaringan komunikasi.
 - (2) Penggunaan teknologi baru.
 - (3) Penggunaan produk baru atau versi terbaru.
 - (4) *Tools* dan lingkungan pengembangan baru.
 - (5) Perubahan lokasi pengerjaan,
 - (6) Perubahan vendor.
- c. Penanggung Jawab Pengelolaan Penyediaan Layanan
- Penanggung jawab pengelolaan penyediaan layanan adalah masing-masing unit kerja penyedia layanan di ANRI.

2. Pengendalian Akses

a. Prasyarat Pengendalian Akses

Prasyarat pengendalian akses mencakup:

- 1) Standar Pengendalian Hak Akses Aplikasi dan Informasi
 - (a) Akses terhadap informasi harus sesuai dengan kewenangan yang dimiliki dan *user id* yang unik.
 - (b) Setiap pengguna sistem wajib menggunakan *user id* dan *password* masing-masing.
 - (c) Pejabat Sistem Keamanan Informasi menetapkan prosedur standarisasi *profil* akses misalnya berupa hak akses administrator dan pengguna pada setiap sistem.
 - (d) Mekanisme untuk kegiatan pengajuan hak akses, otorisasi hak akses, pengadministrasian hak akses, pemantauan hak akses perlu dilakukan secara periodik.
 - (e) Setiap pemilik informasi dan aset pemrosesan informasi bertanggung jawab untuk penyusunan kebijakan pengendalian hak akses.
 - (f) Kebijakan pengendalian akses dapat diwujudkan dengan penyusunan matriks Hak akses guna memetakan pengguna dengan hak akses dan informasi atau aset pengolahan informasi.
 - (g) Pengguna hanya akan diberikan akses informasi ANRI berdasarkan kebutuhan operasional pekerjaannya.
 - (h) Pemberian hak akses terhadap pihak ketiga hanya dapat dilakukan setelah ditandatanganinya perjanjian kerahasiaan.
- 2) Akses ke Jaringan dan Layanan Jaringan
 - (a) Fitur keamanan, tingkat layanan dan kebutuhan terhadap layanan jaringan yang diidentifikasi dalam operasional sistem di ANRI harus dimonitor dan dievaluasi secara berkala.
 - (b) Perangkat milik pribadi tidak diperkenankan terhubung ke jaringan internal ANRI.
 - (c) Seluruh akses kedalam perangkat layanan jaringan ANRI hanya dapat dilakukan oleh pegawai penanggung jawab jaringan yang telah mendapatkan otorisasi dari

unit kerja yang melaksanakan tugas atau fungsi layanan di bidang teknologi informasi dan komunikasi.

- (d) Akses jaringan secara remote harus mendapatkan persetujuan dari unit kerja yang melaksanakan tugas atau fungsi layanan di bidang teknologi informasi dan komunikasi.
- (e) Penggunaan jaringan harus direviu secara berkala melalui *audit log* yang dilakukan untuk mengidentifikasi kejadian atau kelemahan yang dapat menimbulkan kegagalan keamanan (*security breach*).
- (f) Penerapan teknologi pengamanan jaringan, seperti otentifikasi dan enkripsi jaringan sebagai fitur keamanan layanan jaringan di ANRI.
- (g) Pengguna hanya diperbolehkan untuk mengakses jaringan dan layanan jaringan yang diizinkan sesuai area kerjanya.
- (h) Pemberian akses ke jaringan dan layanan jaringan ANRI harus berdasarkan kebutuhan operasional pekerjaan pengguna yang bersangkutan.
- (i) Perhatian lebih dan pengamanan tambahan harus diberikan untuk akses ke jaringan dan layanan jaringan internal ANRI dari jaringan internet (*remote access*).

b. Pengelolaan Akses Pengguna

Prosedur pengelolaan akses pengguna mencakup:

1) Pendaftaran Pengguna dan Penghapusan Hak Akses

- (a) Penerapan proses registrasi dan deregistrasi user untuk perizinan akses ke dalam sistem informasi dan jaringan.
- (b) Pemberian hak akses pengguna harus dilengkapi dengan otentifikasi dan otorisasi serta harus diadministrasikan.
- (c) *User id* harus bersifat unik dan harus menunjukkan identitas nama dengan jelas bagi setiap pengguna dan telah mendapatkan persetujuan dari pimpinan unit.
- (d) Tingkat hak akses yang diberikan kepada pengguna harus sesuai dengan kewenangannya.
- (e) *User id* dan hak akses bagi pegawai ANRI yang telah

berganti fungsi, tugas atau telah meninggalkan lingkungan ANRI harus segera dicabut atau dinonaktifkan.

- (f) Penggunaan *user id* bersama (*shared*) harus dihindari, kecuali untuk kondisi penggunaan tersebut memiliki landasan kewenangan terhadap operasional dan layanan. Penggunaan *user id* bersama harus disetujui secara formal dan didokumentasikan dalam bentuk berita acara.

c. Pemberian Hak Akses Pengguna

- 1) Proses pengadaan untuk memberikan atau mencabut hak akses yang diberikan kepada *user id* meliputi:
 - (a) Persetujuan otorisasi dari pimpinan masing-masing unit kerja ANRI.
 - (b) Verifikasi untuk memastikan tingkat akses yang diberikan telah sesuai dengan kebijakan akses.
 - (c) Hak akses pengguna yang telah rotasi/mutasi/demosi/promosi harus segera disesuaikan dengan posisinya.
 - (d) Hak *user id* yang telah pensiun harus segera dihapus atau diblokir.
 - (e) Reviu pemberian hak akses dilakukan secara berkala.
- 2) Permintaan hak akses harus diajukan secara formal oleh pimpinan unit kerja dan disetujui oleh administrator yang berwenang.
- 3) Persetujuan pemberian hak akses perlu memperhatikan kebutuhan operasional pekerjaan.
- 4) Pemberian hak akses harus direviu secara berkala untuk mengidentifikasi perubahan terhadap pengguna seperti pensiun, promosi, demosi, perpindahan posisi atau terminasi kepegawaian.
- 5) Seluruh proses pemberian dari hak akses tersebut harus didokumentasikan dengan baik.

d. Hak Akses Khusus

- 1) Yang dimaksud dengan hak akses khusus adalah pemberian hak akses untuk keperluan pemeliharaan dan pengujian sistem, serta audit.
- 2) Pemberian dan penggunaan hak akses khusus untuk

informasi (*read and write*) dan sistem informasi (root, administrator) ANRI harus dibatasi dan dikendalikan.

- 3) Proses otorisasi dan catatan dari semua hak akses khusus yang diberikan harus didokumentasikan.
 - 4) Hak akses khusus harus diberikan dalam format *user id* yang berbeda dengan hak akses biasa dan bersifat sementara berdasarkan masa penugasan.
 - 5) Penggunaan hak akses khusus harus dimonitor untuk memastikan tidak adanya akses tanpa izin.
 - 6) Hak akses dengan tujuan untuk pelaksanaan audit terhadap sistem harus diberikan dengan wewenang *read only*.
 - 7) Pengelolaan hak akses khusus perlu memperhatikan beberapa hal berikut:
 - (a) Persetujuan formal untuk hak akses khusus hanya dapat diberikan oleh pemilik dari informasi atau sistem informasi terkait.
 - (b) Pemantauan/peninjauan secara berkala untuk hak akses khusus yang telah dialokasikan.
 - (c) Hak akses khusus yang digunakan secara bersama (*shared*) harus dikontrol untuk mencegah penyalahgunaan melalui *dual custody* dari *password*, penggantian *password* secara berkala atau penggantian *password* segera dilakukan setelah salah satu pemegang *password* berhenti atau mengalami mutasi.
- e. Penerapan Privileged Access Management dan Identity and Access Management.

Dalam rangka memperkuat pengendalian akses terhadap Sistem Elektronik, Aplikasi, Infrastruktur Teknologi Informasi dan Komunikasi, serta aset informasi ANRI, diterapkan pengelolaan identitas dan akses melalui mekanisme Identity and Access Management (IAM) dan/atau Privileged Access Management (PAM) sesuai dengan tingkat risiko, kritikalitas sistem, dan kebutuhan layanan.

Penerapan IAM sebagaimana dimaksud dilakukan untuk memastikan bahwa identitas pengguna, hak akses, peran, otorisasi, autentikasi, perubahan hak akses, penonaktifan

akun, dan pencabutan akses dikelola secara terkendali, terdokumentasi, dan sesuai dengan prinsip kebutuhan akses paling minimum.

Penerapan PAM sebagaimana dimaksud dilakukan untuk mengendalikan, memantau, mencatat, meninjau, dan mengevaluasi penggunaan hak akses istimewa, termasuk namun tidak terbatas pada akun administrator, root, super user, operator sistem, administrator basis data, administrator jaringan, administrator aplikasi, dan akun layanan yang memiliki kewenangan tinggi terhadap Sistem Elektronik dan Infrastruktur Teknologi Informasi dan Komunikasi ANRI.

Pengelolaan akun berhak istimewa paling sedikit mencakup:

1. identifikasi dan inventarisasi akun berhak istimewa;
2. pemberian akses berdasarkan persetujuan pejabat yang berwenang;
3. pembatasan hak akses sesuai tugas, fungsi, dan kebutuhan operasional;
4. penggunaan autentikasi yang kuat;
5. pencatatan dan pemantauan aktivitas akun berhak istimewa;
6. peninjauan hak akses secara berkala;
7. pencabutan atau penonaktifan akses apabila pengguna berubah tugas, mutasi, tidak lagi bekerja, atau tidak lagi memerlukan akses;
8. pelaporan dan tindak lanjut atas penyalahgunaan atau anomali penggunaan hak akses istimewa.

Aktivitas penggunaan akun berhak istimewa harus terekam dalam log audit dan dapat digunakan untuk kebutuhan pemantauan, investigasi, audit, penegakan kepatuhan, dan penanganan insiden keamanan informasi. Penanggung jawab penerapan dan pengelolaan IAM dan/atau PAM adalah unit kerja yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi, dengan melibatkan unit kerja pemilik proses bisnis dan unit kerja terkait sesuai dengan kewenangannya.

f. Hak Akses Pihak Ketiga

Prosedur pengelolaan akses pihak ketiga mencakup:

- 1) Hak akses diajukan oleh pemberi pekerjaan dan atas persetujuan dari pengelola sistem teknologi dan informasi seperti *operating system*, aplikasi, database, atau sistem teknologi informasi lainnya.
- 2) Hak akses kepada pihak ketiga diberikan berdasarkan kontrak dan setelah pihak ketiga menandatangani perjanjian kerahasiaan *non-disclosure agreement*.
- 3) Dalam pengajuan hak akses harus menyebutkan mengenai pekerja pihak ketiga yang diajukan, jangka waktu penggunaan hak akses, dan alasan kebutuhan penggunaan hak akses.
- 4) Hak akses harus berupa *user account* yang dilengkapi dengan *password* sesuai ketentuan.
- 5) Hak akses bersifat sementara dan diberikan hanya pada jangka waktu tertentu.
- 6) Administrator harus mengawasi penggunaan hak akses selama masa berlakunya hak akses tersebut.
- 7) Hak Akses harus dihapus setelah selesai masa berlaku.

g. Pengelolaan Informasi Otentifikasi Rahasia Milik Pengguna

- 1) Informasi otentifikasi rahasia adalah informasi rahasia yang digunakan untuk mengotentifikasikan seorang pengguna pada saat akan mengakses sebuah sistem informasi, diantaranya *password*, *smartcard*, *token*, atau PIN.
- 2) Pemberian informasi otentifikasi rahasia harus dikendalikan melalui proses pengelolaan formal.
- 3) Dalam pengelolaan informasi otentifikasi rahasia harus diperhatikan hal-hal sebagai berikut:
 - (a) Pengguna memahami tanggung jawabnya untuk menjaga keamanan dari informasi otentifikasi yang dimilikinya.
 - (b) Pengguna dilarang memberikan informasi otentifikasi rahasia miliknya kepada pihak lain.
 - (c) Apabila karena alasan yang dibenarkan pengguna terpaksa memberikan informasi otentifikasi rahasia berupa *password* kepada pihak lain, maka pengguna

harus menggantinya pada kesempatan pertama.

- (d) *Password* sementara yang tidak mudah ditebak dapat diberikan kepada pengguna untuk melakukan akses pertama kali ke dalam sistem informasi ANRI. Pengguna harus segera mengganti *password* sementara tersebut.
 - (e) Penyimpanan informasi otentifikasi harus dilakukan secara aman dengan perlindungan yang tepat.
 - (f) Informasi otentifikasi yang bersifat default dari vendor harus segera diganti setelah dilakukan instalasi sistem atau perangkat lunak.
- 4) Seluruh pengguna harus memiliki *user id* yang hanya untuk digunakan secara individu.
 - 5) Penggunaan *user id* secara bersama (*shared*) harus dibatasi dan hanya untuk kondisi dimana perangkat atau sistem yang dijalankan tidak memungkinkan pemisahan *user id*. Penggunaan *user id* secara bersamaan harus mendapatkan persetujuan secara formal dari Pejabat Pimpinan Tinggi Pratama di lingkungan ANRI dan dituangkan dalam berita acara.
- h. Peninjauan Terhadap Hak Akses Pengguna
- 1) Administrator sistem di ANRI harus melakukan peninjauan terhadap hak akses user secara berkala.
 - 2) Peninjauan dilakukan secara reguler, sekali setiap 1 (satu) bulan dan setiap ada perubahan terhadap pengguna.
 - 3) Otorisasi hak akses khusus harus ditinjau secara reguler setelah masa penugasan berakhir.
 - 4) Peninjauan ini merupakan tanggung jawab dari pemilik informasi dan/atau sistem informasi terkait.
 - 5) Perubahan pada hak akses khusus harus didokumentasikan.
- i. Pencabutan atau Penyesuaian Hak Akses
- 1) Hak akses pegawai ANRI harus diblok sebelum ditentukan apakah perlu untuk penghapusan hak akses setelah pemutusan hubungan kerja mereka, atau disesuaikan jika ada perubahan.
 - 2) Beberapa saat sebelum proses pemberhentian atau pergantian status kepegawaian perlu dipertimbangkan untuk membatasi akses terhadap informasi atau sistem

informasi ANRI.

j. Penanggung Jawab Pengelolaan Akses Pengguna

Penanggung jawab pengelolaan akses pengguna adalah unit kerja yang melaksanakan tugas atau fungsi layanan di bidang teknologi informasi dan komunikasi.

k. Standar Tanggung Jawab Pengguna (*User*)

Tanggung jawab pengguna termasuk, namun tidak terbatas pada:

- 1) Setiap pegawai atau pengguna sistem di lingkungan ANRI wajib menggunakan *password* di perangkat yang digunakan dan menjaga kerahasiaan *password* serta menghindari menyimpan catatan *password* di tempat terbuka.
- 2) Setiap pegawai atau pengguna sistem di lingkungan ANRI wajib mengganti *password* apabila terdapat indikasi sistem dan *password* mengalami penyalahgunaan atau kebocoran.
- 3) Penggunaan *password* harus memenuhi kualitas minimal sebagai berikut:
 - a) Panjang minimal karakter *password* pada sistem dan perangkat yang digunakan adalah 8 (delapan) karakter, menggunakan kombinasi huruf dan angka, serta menggunakan spesial karakter (seperti: 1\$%#*) kecuali apabila sistem atau aplikasi tidak memungkinkan untuk hal ini.
 - b) Operasionalisasi sistem yang tidak dapat mengikuti penggunaan *password* dengan kualitas minimum harus mendapatkan persetujuan dari Pimpinan Tinggi Pratama yang melaksanakan tugas atau fungsi layanan di bidang teknologi informasi dan komunikasi dengan mempertimbangkan kendala dan risiko yang ada.
- 4) Memastikan bahwa *password* tidak boleh sama dengan *user id* dan tidak berupa sesuatu yang mudah ditebak, seperti nama, nomor telepon, tanggal lahir, nama anggota keluarga, nama/identitas ANRI.
- 5) Mengganti *password* secara reguler selama 3 (tiga) bulan dengan menghindari menggunakan *password* yang sudah

pernah digunakan.

- 6) Wajib menjaga kerahasiaan *password* dan tidak diperkenankan memberikan *password* kepada orang lain dan/atau menggunakan *password* milik orang lain.
 - 7) Wajib mematuhi kebijakan dan prosedur yang berlaku dalam pemilihan dan penggunaan informasi otentikasi rahasia.
 - 8) Memastikan bahwa otentifikasi rahasia masing-masing telah memenuhi ketentuan-ketentuan sebagai berikut:
 - a) Tidak terdiri dari urutan karakter baik angka, huruf maupun lokasi pada *keyboard*, seperti 12345678, asdfgh, qwerty atau 1234zxcv.
 - b) Penggantian *password* sementara pada saat pertama kali *log-on*.
 - c) Tidak menggunakan atau memasukkan *password* ke sistem secara otomatis.
 - d) Tidak menggunakan *password* yang sama untuk penggunaan bisnis dan pribadi.
 - 9) Memastikan penggunaan *password* telah memenuhi ketentuan - ketentuan sebagai berikut:
 - a) Menggunakan *password* yang mudah diingat, namun tidak mudah ditebak.
 - b) Tidak terdiri dari urutan karakter baik angka, huruf maupun lokasi pada *keyboard*, seperti 12345678, asdfgh, qwerty atau 1234zxcv.
 - c) Mengganti *password* sementara pada saat pertama kali *log on*.
 - d) Tidak menampilkan karakter *password* pada saat *log-on*.
 - e) Tampilan karakter *password* diganti dengan simbol.
 - 10) Administrator pengelola sistem informasi perlu memperhatikan dan mencatat setiap laporan kehilangan informasi otentifikasi rahasia atau permintaan *reset password*.
1. Pengendalian Akses Informasi dan Aplikasi
Hal-hal yang termasuk dalam prosedur pengendalian akses adalah:
 - 1) Pembatasan Akses Informasi

- a) Pembatasan akses ke informasi pada sistem jaringan oleh pengguna sesuai dengan kewenangannya.
- b) Pembatasan akses dilakukan berdasarkan kebutuhan pegawai dan sesuai dengan keperluan operasional dan layanan pegawai tersebut.
- c) Pembatasan akses dilakukan antara lain dengan pengendalian hak untuk *read*, *write*, *copy* maupun *delete*.

2) Prosedur *Log-On* secara Aman

Akses ke sistem operasi harus dikontrol dengan menggunakan mekanisme *secure log-on* meliputi:

- a) Tidak memberikan pesan bantuan yang dapat menyebabkan *log on* tanpa izin.
- b) Pembatasan jumlah kesalahan dalam percobaan *log-on* dan apabila jumlah kesalahan maksimal telah terlewati, dilakukan penerapan hal-hal berikut:
 - (1) perekaman setiap percobaan *log on* baik yang gagal maupun berhasil.
 - (2) pemberian jeda waktu sebelum *log-on* dapat dilakukan kembali atau menolak percobaan kembali setelah terjadi kesalahan dalam percobaan *log-on*.
 - (3) pemutusan koneksi data.
 - (4) penyampaian pesan peringatan pada sistem bahwa jumlah maksimal percobaan *log-on* telah terlewati.
 - (5) jumlah maksimal percobaan *log-on* perlu mempertimbangkan panjang minimal dari *password* dan nilai sistem yang dilindungi.
- c) Tidak menampilkan karakter *password* pada saat *log-on*. Tampilan karakter *password* dapat diganti dengan simbol.
- d) Tidak memberikan petunjuk mengenai sistem atau aplikasi sebelum proses *log-on* telah sukses dilakukan.
 - (1) Penyampaian peringatan, bahwa sistem atau aplikasi hanya boleh diakses oleh orang yang berkepentingan.
 - (2) Validasi informasi *log-on* hanya setelah seluruh

data telah dimasukkan ke dalam proses *log-on*. Apabila terjadi kesalahan input data pada proses *log-on*, sistem tidak boleh mengindikasikan bagian data mana yang salah.

- (3) Pembatasan waktu minimal dan maksimal untuk proses *log-on*.
- (4) Setelah proses *log on* yang berhasil sistem perlu menampilkan waktu dari proses *log-on* terakhir, baik yang berhasil maupun yang gagal.
- (5) Tidak mentransmisikan *password* dalam *clear text* melalui jaringan.

3) Sistem Pengelolaan *Password*

- a) Sistem pengelolaan *password* harus memastikan bahwa penggantian *password* dilakukan secara reguler yaitu maksimal 3 (tiga) bulan sekali.
- b) Sistem untuk mengelola *password* perlu bersifat interaktif dan harus dapat memastikan kualitas *password* pengguna sistem informasi ANRI.
- c) Sistem pengelolaan *password* harus memastikan:
 - (1) Penggunaan *user id* dan *password* individual untuk setiap pegawai.
 - (2) Pengguna dapat mengganti *password* nya.
 - (3) Penggunaan *password* yang sesuai dengan aturan terkait penggunaan *password*.
 - (4) Pengguna mengganti *password* sementara pada saat *log-on* untuk pertama kali.
 - (5) Tidak menampilkan *password*.
 - (6) Penyimpanan *file* yang berisi *password* secara terpisah dari data aplikasi.
 - (7) Penyimpanan dan pengiriman *password* dilakukan dengan menggunakan perlindungan khusus seperti enkripsi dan *hashing*.

4) Penggunaan Program Utilisasi Khusus.

- a) Penggunaan *system utility* program yang berpotensi dapat mengambil alih pengendalian sistem jaringan harus dibatasi dan dikendalikan secara ketat.
- b) Administrator jaringan harus melakukan proses

identifikasi, otentifikasi dan otorisasi untuk seluruh *system utilities* yang digunakan dan membatasi penggunaan *system utilities*.

- c) Penggunaan *system utility* harus diberikan hanya kepada personel yang memiliki kebutuhan operasional yang valid dan harus disetujui oleh pemilik dari sistem yang diaksesnya.

5) Pengendalian Akses ke Kode Sumber Program

- a) Akses ke *source code* program beserta dokumentasi terkait lainnya seperti desain, spesifikasi, verifikasi dan validasi, harus dikendalikan secara ketat untuk mencegah akses tanpa izin. Hal ini dapat dilakukan melalui penyimpanan *source code* secara terpusat.
- b) Pengendalian akses ke *source code* program harus memperhatikan:
 - (1) Penyimpanan *source code* tidak dilakukan pada sistem operasional.
 - (2) Implementasi kontrol akses *source code*.
 - (3) Pengaksesan *source code* harus melalui otorisasi formal.
 - (4) Penyiapan dan pemeliharaan daftar *source code*.
 - (5) Dokumentasi dan pencatatan *audit log* setiap akses ke *source code* program.
 - (6) Pemeliharaan dan penyalinan *source code* program harus dilakukan melalui mekanisme pengendalian perubahan.

- 6) Penanggung Jawab Pengendalian Akses Informasi dan Aplikasi Penanggung jawab pengendalian akses informasi dan aplikasi adalah unit kerja yang melaksanakan tugas atau fungsi layanan di bidang teknologi informasi dan komunikasi.

3. Kriptografi

- a. Pengelolaan Kriptografi meliputi:

- 1) Kebijakan Penggunaan Kriptografi

- a) Penggunaan teknologi kriptografi dapat digunakan untuk melindungi informasi milik ANRI.
- b) Implementasi kriptografi perlu mempertimbangkan aspek hukum dan regulasi negara yang mungkin membatasi penggunaan kriptografi terutama untuk

pengiriman antarnegara.

- c) Keputusan penggunaan teknologi kriptografi perlu menimbang sensitivitas (sisi kerahasiaan) dan kritikalitas (sisi integritas) dari informasi yang akan dilindungi.
- d) Penggunaan enkripsi harus dipertimbangkan untuk melindungi informasi sensitif dan/atau rahasia yang dipindahtangankan atau dikirimkan baik melalui media jaringan informasi.
- e) Setiap sistem jaringan harus mempertimbangkan penggunaan kriptografi yang mencakup tipe, kekuatan dan kualitas dari algoritma Kriptografi yang digunakan pada jaringan. Algoritma kriptografi yang sudah terbukti dapat dipecahkan dengan mudah tidak boleh digunakan di lingkungan ANRI.
- f) Pada proses pengembangan sistem aplikasi yang mengolah informasi rahasia implementasi enkripsi digunakan untuk pengamanan terhadap informasi yang dihasilkan dan dipertukarkan sehingga terhindar dari akses ilegal dan pencurian informasi oleh pihak-pihak tertentu.
- g) Penerapan enkripsi untuk memastikan keamanan informasi rahasia dalam proses pertukarannya pada arca sistem jaringan.
- h) Pertukaran informasi rahasia yang menggunakan media *e-mail* harus memenuhi hal berikut:
 - (1) Penerapan *message integrity check* untuk memastikan isi beserta *attachment e-mail* tidak diubah oleh pihak yang tidak berwenang selama dalam perjalanan.
 - (2) Penerapan *digital signature* untuk menghindari penolakan (*repudiation*).
- i) Penerapan enkripsi harus dilakukan untuk melindungi data yang berasal dari *production system* dan bersifat rahasia sebelum digunakan sebagai *testing* data pada *environment* UAT. Penggunaan data *scrambling* (pengacakan data) dapat dibenarkan sebagai alternatif untuk melindungi kerahasiaan data asli sebelum

digunakan sebagai data *testing*.

j) Penggunaan *proprietary* enkripsi yang belum teruji keandalannya harus dihindari.

k) Enkripsi yang disarankan untuk diterapkan dalam penyimpanan informasi yang bersifat rahasia adalah dengan panjang key minimal 128 bit dengan alternatif algoritma:

(1) *Advanced Encryption Standard* (AES).

(2) 3DES (*Triple Data Encryption Standard*).

(3) Algoritma lainnya yang menggunakan panjang key minimal 128 bit.

l) Penerapan enkripsi pada protokol komunikasi berupa SSL/HTTPS pada sistem aplikasi *web based* dapat dibenarkan apabila enkripsi pada penyimpanan informasi belum memungkinkan.

2) Manajemen dari *Key* untuk Kebutuhan Kriptografi

a) Seluruh *key* kriptografi harus dilindungi dari modifikasi, kehilangan serta kerusakan.

b) Sistem manajemen dari *key* kriptografi harus berdasar pada mekanisme pengelolaan *key* yang memadai.

c) Peralatan yang digunakan untuk menghasilkan dan menyimpan *key* kriptografi harus dilindungi secara fisik.

d) Pengelolaan dari *key* kriptografi harus dikendalikan secara ketat dan dibatasi hanya pada personel yang terotorisasi. Apabila memungkinkan, pengelolaan dari *key* kriptografi didasarkan pada prinsip *dual custody* untuk mengurangi risiko penyalahgunaan.

e) Apabila terdapat indikasi kebocoran *key* kriptografi, maka *key* tersebut harus segera dicabut dan diganti.

3) Regulasi Terkait Kriptografi

Penggunaan dan pengelolaan teknik kriptografi harus sesuai dengan regulasi terkait kriptografi yang berlaku di Indonesia.

4) Penanggung Jawab Pengelolaan Kriptografi

Penanggung jawab pengendalian adalah unit kerja yang melaksanakan tugas atau fungsi layanan di bidang teknologi informasi dan komunikasi.

4. Pengelolaan Keamanan Perangkat Lunak Operasional

Pengelolaan proses instalasi perangkat lunak pada sistem operasional mencakup:

- a. Pengendalian instalasi *software* pada sistem operasional (*production*) di ANRI
- b. Pengendalian terhadap sistem operasional meliputi:
 - 1) Sistem *production* hanya mengoperasikan sistem yang telah disetujui oleh pejabat yang berwenang dan tidak digunakan untuk menjalankan aplikasi yang masih dalam tahap pengembangan.
 - 2) Pendokumentasian konfigurasi sistem operasional dan pembaruan setiap perubahan.
 - 3) Proses pembaruan perangkat lunak, aplikasi dan *library* pada sistem *production* hanya boleh dilakukan oleh pegawai yang diberi wewenang setelah mendapatkan otorisasi dari pihak yang berwenang.
 - 4) Aplikasi dan sistem operasi hanya dapat di-*install* pada sistem *production* setelah melalui proses pengujian. Proses pengujian mencakup namun tidak terbatas pada pengujian fungsi, kegunaan, keamanan serta dampak terhadap sistem lain.
 - 5) Penggunaan sistem pengendalian konfigurasi guna memonitor dan mengendalikan seluruh aplikasi yang di-*install* pada sistem *production* beserta dokumentasinya.
 - 6) Penerapan strategi *rollback* sebelum setiap dilakukan perubahan pada sistem *production*.
 - 7) Pemeliharaan *audit log* untuk semua *update* pada sistem *production*.
 - 8) Penyimpanan versi lama dari aplikasi yang telah di-*install* pada sistem *production* beserta dengan dokumentasi sistem aplikasi yang mencakup namun tidak terbatas pada parameter, prosedur, konfigurasi serta aplikasi pendukung lainnya.
- c. Kepastian jaminan vendor penyedia atas dukungan operasional selama jangka waktu digunakannya aplikasi pada sistem *production*.
- d. Setiap keputusan untuk melakukan *upgrade* aplikasi harus mempertimbangkan kebutuhan layanan serta keamanan

informasi pada versi yang baru.

- e. Akses secara fisik maupun non fisik diberikan kepada vendor untuk keperluan pemeliharaan sistem dan/atau aplikasi hanya setelah mendapatkan persetujuan dari pejabat yang berwenang.
- f. Pengawasan atas semua aktivitas akses vendor.
- g. Penanggung Jawab Pengelolaan Keamanan Perangkat Lunak Operasional.

Penanggung jawab pengelolaan keamanan perangkat lunak operasional adalah unit kerja yang melaksanakan tugas atau fungsi layanan di bidang teknologi informasi dan komunikasi.

5. Pengelolaan Persyaratan Keamanan Sistem Informasi

Pengelolaan persyaratan keamanan sistem informasi mencakup:

- a. Analisis dan penentuan spesifikasi kebutuhan keamanan dalam sistem informasi
 - 1) Setiap perubahan sistem baru maupun perbaikan sistem yang sudah ada harus mempertimbangkan kebutuhan pengendalian keamanan.
 - 2) ANRI harus melakukan proses pengujian sistem yang disediakan vendor penyedia untuk menjamin terpenuhinya seluruh kebutuhan keamanan dalam sistem informasi.
 - 3) Proses pengujian dan akuisisi harus mempertimbangkan fungsi keamanan sistem informasi yang disediakan serta risiko yang mungkin muncul dalam penggunaan sistem informasi dari vendor tertentu.
 - 4) Penyusunan spesifikasi kebutuhan keamanan informasi perlu memperhatikan implementasi kontrol keamanan. Hal ini perlu diterapkan untuk setiap perangkat lunak aplikasi layanan dan penunjangnya.
 - 5) Persyaratan keamanan dalam sistem informasi harus mempertimbangkan kebutuhan dan risiko dari layanan serta dampak yang mungkin timbul dari kegagalan keamanan dalam sistem informasi.
 - 6) Penyusunan spesifikasi kebutuhan keamanan dalam sistem informasi harus dilakukan pada fase awal pengembangan sistem informasi untuk memastikan

kemudahan implementasi keamanan dalam sistem informasi.

b. Mengamankan Sistem Aplikasi pada Jaringan publik

- 1) Informasi yang digunakan oleh sistem aplikasi yang dikirimkan melalui jaringan publik harus diamankan untuk menghindari *dispute*, kebocoran dan perubahan tanpa izin.
- 2) Pengamanan tersebut perlu mempertimbangkan aspek-aspek berikut:
 - (a) Kepastian identitas dari pihak-pihak yang terlibat dalam pertukaran informasi melalui aplikasi pada jaringan publik.
 - (b) Kepastian integritas dari informasi yang dipertukarkan.
 - (c) Kepastian kerahasiaan dari informasi yang dipertukarkan.
 - (d) Kepastian tidak terjadinya duplikasi dari informasi yang dipertukarkan.
 - (e) Penggunaan teknologi otentikasi dan enkripsi yang memadai untuk proses pengamanan informasi tersebut.
- 3) Pengamanan yang diimplementasikan perlu selaras dengan sensitivitas informasi yang dipertukarkan dan risiko yang ada.

c. Melindungi pertukaran informasi yang dilakukan oleh sistem aplikasi

- 1) Informasi yang dipertukarkan oleh sistem aplikasi harus diamankan untuk mencegah risiko transmisi yang tidak lengkap, kebocoran, perubahan dan perulangan informasi tanpa otorisasi.
- 2) Penggunaan teknologi otentikasi dan enkripsi yang memadai untuk proses pengamanan informasi dan jalur komunikasi yang digunakan untuk pertukaran.
- 3) Pengamanan yang diimplementasikan selaras dengan sensitivitas informasi yang dipertukarkan dan risiko yang ada.
- 4) Penanggung Jawab Pengelolaan Persyaratan Keamanan Sistem Informasi.

Penanggung jawab pengelolaan persyaratan keamanan sistem informasi adalah adalah unit kerja yang

melaksanakan tugas atau fungsi layanan di bidang teknologi informasi dan komunikasi.

6. Pengelolaan Keamanan pada Proses Pengembangan dan *Support*
Pengelolaan keamanan pada proses pengembangan dan *support* meliputi:

a. Kebijakan Keamanan dalam Pengembangan Sistem Informasi

1) Penetapan dan implementasi aturan untuk memastikan keamanan dalam proses pengembangan dan pemberian dukungan (*support*) sistem informasi;

2) Pengembangan desain kendali keamanan harus memenuhi persyaratan kepatuhan kepada peraturan perundangan tentang standar teknis keamanan informasi;

3) Aturan proses pengembangan sistem harus mempertimbangkan hal-hal sebagai berikut:

a) Telah mendapatkan rekomendasi evaluasi anggaran (*clearance*) oleh unit kerja yang melaksanakan tugas atau fungsi layanan di bidang teknologi informasi dan komunikasi/lembaga yang berwenang.

b) Pengamanan dari lingkungan pengembangan, pemisahan lingkungan pengembangan baik secara fisik dan/atau non fisik.

c) Pengendalian akses.

d) Penyediaan panduan keamanan dalam melakukan *coding*.

e) Pengendalian versi aplikasi.

f) Penyimpanan *source code*.

g) Penerapan metode pengujian untuk mengidentifikasi dan memperbaiki *vulnerability*. Jika pengembangan *software* dan sistem menggunakan metode alih daya (*outsourced*), maka harus memperhatikan:

(1) Perjanjian terkait lisensi dan kepemilikan sistem.

(2) Pengujian terhadap penerimaan sistem.

(3) Prasyarat dokumentasi untuk sistem.

(4) Perjanjian escrow.

(5) Hak melakukan audit pada proses pengembangan dan kontrol yang diimplementasikan oleh vendor.

(6) Pemberian dukungan (*support*) terhadap sistem informasi yang dikembangkan meliputi pemeliharaan dan implementasi sistem.

- b. Prosedur Pengendalian Perubahan (*change*) Sistem Informasi
- 1) Pengendalian implementasi perubahan sistem informasi dengan menerapkan prosedur formal pengendalian perubahan.
 - 2) Penerapan prosedur formal bertujuan untuk mengurangi kemungkinan terjadinya kesalahan atau kerusakan pada sistem informasi ANRI.
 - 3) Setiap pengembangan baru atau perubahan pada sistem yang sudah ada harus mengikuti proses pengendalian perubahan.
 - 4) Prosedur pengendalian perubahan mencakup proses penilaian risiko, analisis terhadap dampak dari perubahan serta spesifikasi dari kontrol keamanan yang dibutuhkan.
 - 5) Prosedur pengendalian harus memastikan bahwa sistem keamanan dan kontrol keamanan tidak mengalami perubahan yang dapat mengganggu keamanan dari sistem.
 - 6) Pengendalian perubahan harus mempertimbangkan beberapa hal berikut:
 - a) Pendokumentasian tingkat otorisasi untuk persetujuan perubahan.
 - b) Kepastian bahwa perubahan hanya diajukan oleh pemilik bisnis proses layanan.
 - c) Peninjauan kontrol keamanan sistem informasi untuk menjamin bahwa perubahan yang dilakukan tidak memengaruhi kontrol tersebut.
 - d) Identifikasi dari semua komponen sistem informasi yang akan mengalami perubahan serta sistem lain yang mungkin terkena pengaruh.
 - e) Jaminan bahwa dokumentasi sistem informasi diperbaharui mengikuti perubahan pada sistem, termasuk menyimpan dokumentasi lama yang sudah tidak berlaku.
 - f) Pengendalian perubahan versi dari sistem informasi yang mengalami perubahan.
 - g) Pemeliharaan *audit trail* untuk setiap langkah dalam proses perubahan sistem.

- h) Jaminan bahwa proses implementasi perubahan dilakukan pada saat yang tepat dan tidak mengganggu proses layanan yang berjalan.
- i) Pengujian terhadap perubahan terhadap sistem, termasuk instalasi *patch* dan *update*, harus dilakukan pada lingkungan yang berbeda dengan lingkungan *production*.
- c. Peninjauan teknis sistem informasi pada saat terjadi perubahan pada *platform* operasional
 - 1) Jika terjadi perubahan *platform* operasinya (sistem operasi, *middleware*, *database*), maka sistem informasi yang kritikal harus ditinjau dan diuji kembali untuk memastikan tidak ada dampak yang dapat mengganggu operasional maupun keamanan informasi sistem tersebut.
 - 2) Perubahan pada *platform* operasi, termasuk perubahan versi dan instalasi *patch* atau *update* harus dikelola untuk memastikan bahwa sistem informasi tidak terkena dampak negatif dari perubahan tersebut.
 - 3) Proses pengelolaan pada nomor 6 poin b tersebut mencakup namun tidak terbatas pada:
 - a) Peninjauan pada kontrol keamanan dan integritas pada sistem informasi.
 - b) Pengalokasian sumber daya, termasuk pegawai, waktu dan biaya, untuk melaksanakan peninjauan dan pengujian sistem yang disebabkan oleh perubahan pada sistem operasi.
 - c) Jaminan bahwa proses perubahan pada SISTEM OPERASI menyediakan waktu yang cukup untuk pengujian dan peninjauan atas aplikasi.
 - 4) Pembatasan Perubahan atau Modifikasi Pada Perangkat Lunak
 - a) Modifikasi pada paket *software* sebaiknya tidak dilakukan atau hanya dibatasi pada perubahan yang sangat dibutuhkan. Selain itu semua perubahan harus dikendalikan dengan ketat.
 - b) Perubahan atau modifikasi perangkat lunak yang di-*supply* oleh pihak ketiga harus dibatasi. Jika perubahan harus dilakukan maka perlu mempertimbangkan hal-hal sebagai berikut:

- (1) Risiko berubahnya proses pengendalian integritas input, proses serta output yang sudah berjalan dalam aplikasi.
 - (2) Bahwa dengan perubahan tersebut, ANRI bertanggung jawab dalam proses pemeliharaan aplikasi di masa mendatang.
 - c) Apabila proses perubahan dan modifikasi perangkat lunak dilakukan, maka versi perangkat lunak sebelum dan sesudah perubahan perlu disimpan dan setiap perubahan yang dilakukan perlu didokumentasikan.
 - d) Setiap perubahan atau modifikasi perlu diuji, divalidasi dan didokumentasikan oleh pengembang sistem informasi.
- d. Rekayasa Sistem Elektronik yang Aman
- 1) ANRI harus menetapkan, mendokumentasikan, memelihara, dan mengimplementasikan fitur-fitur keamanan dalam melakukan rekayasa sistem informasi agar menghasilkan suatu sistem yang aman.
 - 2) Fitur keamanan harus diimplementasikan pada seluruh komponen sistem informasi yang mencakup namun tidak terbatas pada perangkat keras, perangkat lunak, sistem operasi, *database* pada *middleware*.
 - 3) Pemilihan fitur keamanan sistem informasi harus dilakukan berdasarkan proses *assessment* risiko dengan memperhitungkan sensitivitas dan kritikalitas sistem dan informasi yang diproses.
 - 4) Fitur keamanan yang perlu dipertimbangkan mencakup namun tidak terbatas pada:
 - a) Metode otentikasi pengguna.
 - b) Metode pengamanan komunikasi dan *session* sistem.
 - c) Metode untuk validasi informasi.
 - d) Metode pengamanan informasi yang diproses dan/atau dipertukarkan oleh sistem berdasarkan sensitivitas dan kritikalitasnya.
- e. Keamanan Lingkungan Pengembangan Sistem Informasi
- 1) ANRI harus mengamankan lingkungan yang digunakan untuk pengembangan sistem informasi dalam setiap tahap pada siklus pengembangan.

- 2) Pengelolaan Akses Berdasarkan Siklus Hidup Arsip. Hak akses terhadap arsip digital harus dikaitkan dengan status siklus hidup arsip, sebagai contoh arsip inaktif atau permanen hanya dapat diakses oleh pihak berwenang, dan harus dilindungi dari akses yang tidak sah.
- 3) Prinsip dalam menetapkan keamanan lingkungan tersebut harus memperhatikan:
 - a) Pengamanan informasi yang digunakan dalam proses pengembangan sistem informasi.
 - b) Pengendalian akses ke lingkungan pengembangan.
 - c) Pemisahan lingkungan pengembangan dengan lingkungan pengujian dan operasional.
 - d) Penerapan *backup* data dan perangkat lunak yang digunakan di lingkungan pengembangan.
 - e) Pemisahan secara fisik, non fisik, maupun pengguna antara lingkungan pengembangan, pengujian, dan operasional.
 - f) Pengendalian perpindahan informasi antarlingkungan pengembangan, pengujian, dan operasional.
- f. Pengembangan Perangkat Lunak Secara *Outsource*
 - 1) Pengembangan perangkat lunak yang dilakukan oleh pihak ketiga harus diawasi dan dipantau.
 - 2) Pengembangan perangkat lunak secara *outsource* perlu mempertimbangkan beberapa hal berikut:
 - a) Kesepakatan mengenai lisensi, kepemilikan *source code* serta hak atas kekayaan intelektual.
 - b) Sertifikasi terkait kualitas dan akurasi dari pekerjaan pengembangan yang dilakukan.
 - c) Kesepakatan mengenai *escrow* apabila terjadi kesalahan atau kegagalan pada pekerjaan pengembangan oleh pihak ketiga.
 - d) Hak untuk melakukan audit terhadap kualitas dan akurasi pekerjaan yang dilakukan.
 - e) Audit dan Penilaian Kesesuaian Berkala. Audit internal dan eksternal dilaksanakan secara berkala untuk memastikan kesesuaian dengan kebijakan, prosedur, dan standar yang berlaku. Hasil audit dijadikan dasar

perbaikan berkelanjutan.

- f) Syarat dalam kontrak mengenai kualitas dan keamanan aplikasi.
- g) Serangkaian pengujian sebelum instalasi dilakukan untuk mendeteksi *malicious code*.

g. Pengujian Keamanan Sistem Informasi

- 1) ANRI dan/atau unit kerja yang mengembangkan aplikasi wajib melakukan pengujian sistem informasi, baik dalam proses pengembangan baru maupun *upgrade* sistem.
- 2) Pengujian dilakukan untuk memastikan seluruh prasyarat terkait fitur keamanan informasi yang telah ditetapkan telah berfungsi sesuai dengan harapan.
- 3) Pengujian keamanan sistem informasi harus dilakukan oleh pegawai yang memiliki kompetensi untuk melakukan hal tersebut.

h. Standar Kontrol Teknis Keamanan Aplikasi

Dalam rangka memastikan keamanan aplikasi yang dikembangkan, dikelola, digunakan, dan/atau dioperasikan oleh ANRI, setiap Aplikasi SPBE dan/atau aplikasi pendukung layanan ANRI wajib menerapkan standar kontrol teknis keamanan aplikasi sesuai dengan tingkat risiko, klasifikasi informasi, kategori Sistem Elektronik, tingkat vitalitas Sistem Elektronik, kebutuhan layanan, dan ketentuan peraturan perundang-undangan.

Standar kontrol teknis keamanan aplikasi sebagaimana dimaksud paling sedikit mencakup:

- 1) kontrol autentikasi, termasuk verifikasi identitas pengguna, pengamanan kata sandi, pembatasan percobaan masuk, pemulihan akun, dan penguatan autentikasi sesuai risiko;
- 2) kontrol manajemen sesi, termasuk pengaturan token sesi, masa berlaku sesi, penghentian sesi, perlindungan cookie, dan pencegahan penggunaan sesi yang tidak sah;
- 3) kontrol akses dan otorisasi, termasuk penerapan prinsip hak akses paling minimum, pemisahan peran, validasi otorisasi pada sisi server, dan pencegahan akses tidak sah terhadap objek atau fungsi aplikasi;
- 4) kontrol validasi input dan output, termasuk validasi, sanitasi, dan pembatasan input untuk mencegah serangan injeksi, cross-site scripting, dan penyalahgunaan parameter aplikasi;

- 5) kontrol kriptografi, termasuk penggunaan algoritma, protokol, modul, dan kunci kriptografi yang aman serta sesuai dengan ketentuan peraturan perundang-undangan;
- 6) kontrol penanganan error dan pencatatan log, termasuk pembatasan informasi teknis yang ditampilkan kepada pengguna, pencatatan kejadian keamanan, perlindungan log, dan dukungan audit trail;
- 7) kontrol proteksi data, termasuk perlindungan data pribadi, data rahasia, metadata, dokumen elektronik, dan informasi sensitif yang diproses, disimpan, ditampilkan, atau dikirimkan melalui aplikasi;
- 8) kontrol keamanan komunikasi, termasuk penggunaan protokol komunikasi yang aman, perlindungan transmisi data, pengamanan TLS/HTTPS, dan menonaktifkan protokol yang tidak aman;
- 9) kontrol pengendalian kode berbahaya, termasuk pencegahan unggahan file berbahaya, validasi tipe dan ukuran file, pemindaian malware, serta pembatasan eksekusi file yang tidak sah;
- 10) kontrol logika bisnis, termasuk validasi alur proses bisnis, pencegahan penyalahgunaan fungsi aplikasi, dan pengujian terhadap bypass proses yang tidak sah;
- 11) kontrol keamanan file, termasuk pengamanan proses unggah, unduh, penyimpanan, akses, penghapusan, dan validasi file;
- 12) kontrol keamanan API dan web service, termasuk autentikasi dan otorisasi API, pembatasan akses endpoint, validasi request dan response, rate limiting, pengamanan token, serta pencatatan aktivitas API;
- 13) kontrol keamanan konfigurasi, termasuk hardening konfigurasi aplikasi, server aplikasi, framework, library, dependency, environment, dan komponen pendukung aplikasi; dan
- 14) kontrol keamanan aplikasi mobile, dalam hal aplikasi disediakan melalui perangkat bergerak, termasuk pengamanan komunikasi, penyimpanan lokal, autentikasi, otorisasi, session/token, serta proteksi terhadap modifikasi dan penyalahgunaan aplikasi.

Pengembangan, perubahan, pemeliharaan, dan pengoperasian

aplikasi harus memastikan bahwa standar kontrol teknis keamanan aplikasi sebagaimana dimaksud telah dirancang, diimplementasikan, diuji, didokumentasikan, dan dievaluasi sebelum aplikasi digunakan pada lingkungan produksi.

Pengujian terhadap kontrol teknis keamanan aplikasi dilakukan melalui mekanisme yang sesuai dengan kebutuhan dan tingkat risiko, antara lain *reviu desain keamanan*, *reviu kode sumber*, *vulnerability assessment*, *penetration testing*, pengujian konfigurasi, pengujian API/web service, pengujian aplikasi mobile, dan/atau pengujian keamanan lainnya.

Setiap kelemahan atau kerentanan keamanan aplikasi yang ditemukan wajib ditindaklanjuti melalui proses perbaikan, pengujian ulang, pencatatan, pelaporan, dan pemantauan sampai dinyatakan selesai sesuai dengan tingkat risiko dan prioritas penanganan.

Penanggung jawab penerapan standar kontrol teknis keamanan aplikasi adalah unit kerja yang mengembangkan, mengelola, dan/atau menggunakan aplikasi bersama unit kerja yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi, serta pihak ketiga apabila pengembangan, pemeliharaan, atau pengoperasian aplikasi melibatkan pihak ketiga.

i. Pengujian Penerimaan Sistem

- 1) Pengujian penerimaan sistem harus ditetapkan sesuai dengan kriteria sistem informasi baru, upgrade dan versi baru.
- 2) Pengujian penerimaan sistem harus mencakup pengujian kebutuhan keamanan informasi dan kepatuhan untuk mengamankan pengembangan sistem.
- 3) Pengujian harus dilakukan pada komponen yang diterima dan sistem terpadu.
- 4) Seluruh *requirement* dan kriteria penerimaan sistem baru harus didefinisikan dengan jelas, disetujui, didokumentasikan, dan diuji.
- 5) Migrasi sistem dari lingkungan pengembangan ke lingkungan *production* hanya dapat dilakukan setelah melalui proses pengujian dan penerimaan sistem secara formal yang memperhatikan hal-hal berikut:
 - a) Spesifikasi kebutuhan dan kinerja infrastruktur sistem

informasi.

- b) Prosedur untuk pemulihan dari kegagalan (*error recovery*), *restart*, serta rencana dalam kondisi darurat (*contingency plan*).
- c) Persiapan dan pengujian prosedur/manual operasional.
- d) Keterlibatan pengguna dalam pengujian sistem.
- e) Persetujuan formal untuk penerimaan hasil pengujian sistem informasi.
- f) Pelatihan untuk penggunaan sistem baru.

j. Penanggung Jawab Pengelolaan Keamanan pada Proses Pengembangan dan *Support*

Penanggung jawab pengelolaan keamanan pada proses pengembangan dan *support* adalah adalah unit kerja yang melaksanakan tugas atau fungsi layanan di bidang teknologi informasi dan komunikasi.

7. Pengelolaan Perlindungan Data untuk Pengujian Sistem Informasi
Pengelolaan perlindungan data untuk pengujian sistem informasi meliputi:

- a. Data untuk pengujian sistem harus dipilih secara hati-hati untuk menghindari pengungkapan dan/atau perubahan informasi sensitif oleh pihak yang tidak berhak serta melindungi dari kemungkinan kerusakan dan kehilangan informasi.
- b. Setiap akun pengguna atau sistem yang digunakan dalam melakukan pengujian sistem dikontrol dan dipantau untuk memastikan bahwa akun tersebut hanya digunakan untuk tujuan yang sah, dan dihapus atau dikembalikan ke fungsi normal setelah pengujian selesai dilakukan.
- c. Data operasional yang digunakan untuk keperluan pengujian harus di masking atau diacak untuk mengaburkan data yang sebenarnya.
- d. Data operasional yang digunakan untuk keperluan pengujian harus dihapus segera setelah proses pengujian telah selesai dilaksanakan.
- e. Untuk melindungi data operasional yang akan digunakan untuk kebutuhan pengujian sistem perlu mempertimbangkan beberapa hal sebagai berikut:
 - 1) Prosedur pengendalian akses yang berlaku untuk sistem

production juga diberlakukan pada sistem untuk pengujian.

- 2) Diperlukan proses persetujuan formal untuk penyalinan (*copy*) dan penggunaan data operasional sebelum digunakan untuk memenuhi kebutuhan pengujian sistem.
- 3) Penyalinan (*copy*) dan penggunaan data operasional perlu didokumentasikan dengan baik.

f. Penanggung Jawab Pengelolaan Perlindungan Data untuk Pengujian Sistem Informasi

Penanggung jawab pengelolaan perlindungan data untuk pengujian sistem informasi adalah adalah unit kerja yang melaksanakan tugas atau fungsi layanan di bidang teknologi informasi dan komunikasi.

8. *Secure Coding*

Prinsip *secure coding* adalah praktik pengembangan perangkat lunak yang dirancang untuk mengidentifikasi dan mengurangi kerentanan keamanan yang dapat dieksploitasi. Prinsip *secure coding* yang diterapkan meliputi:

- a. Setiap pembangunan, pengembangan, integrasi, perubahan, dan pemeliharaan Aplikasi wajib menerapkan Secure Software Development Life Cycle secara proporsional berdasarkan risiko, sejak perencanaan sampai dengan penghentian layanan.
- b. Seluruh data yang diterima oleh aplikasi harus diverifikasi dan divalidasi dengan cermat. Hal ini membantu mencegah serangan umum seperti *injection attacks* (misalnya, *SQL injection*) atau *cross-site scripting* (XSS).
- c. Pengembang perangkat lunak harus menghindari penggunaan kerentanan umum dalam pemrograman, seperti *buffer overflow* atau penggunaan fungsi yang tidak aman. Hal ini dapat dicapai dengan menggunakan *library* dan *framework* yang aman, menghindari penggunaan fungsi yang sudah usang atau tidak aman, dan melakukan validasi parameter fungsi secara teliti.
- d. Setiap pengembang atau entitas yang mengakses sistem harus melalui proses autentikasi yang kuat. Pengguna juga harus diberikan akses hanya pada fungsi dan data yang sesuai dengan tingkat otorisasi mereka. Prinsip ini membantu mencegah serangan seperti *brute-force attacks* atau *privilege*

escalation.

- e. *Session management* harus diimplementasikan dengan baik untuk mencegah serangan seperti *session hijacking* atau *session fixation*. *Session* harus dienkripsi, memiliki waktu kadaluarsa, dan menggunakan mekanisme yang kuat untuk menghasilkan *session ID*.
 - f. Pengembang perangkat lunak harus melibatkan pengujian keamanan secara teratur untuk mengidentifikasi kerentanan dan celah keamanan yang mungkin ada dalam perangkat lunak. Pengujian keamanan dapat meliputi pengujian penetrasi, pengujian *fuzzing*, dan analisa kode statis. Pengembang dan pihak yang terlibat perlu terus memperbarui pengetahuan tentang kerentanan keamanan dan mengikuti praktik terbaik dalam *secure coding*. Penggunaan *framework* atau *library* yang diperbarui secara teratur juga dapat membantu mengurangi risiko keamanan.
- Kebijakan teknis aplikasi akan ditetapkan oleh Pimpinan Tinggi Pratama yang melaksanakan tugas atau fungsi layanan di bidang teknologi informasi dan komunikasi.

BAB III

PENETAPAN PENANGGUNG JAWAB

Bahwa dalam rangka untuk menunjang Sistem Manajemen Keamanan Informasi diperlukan:

A. Komitmen Pimpinan

Komitmen pimpinan sebagaimana dimaksud diwujudkan dengan:

1. Memastikan sistem manajemen keamanan informasi dilaksanakan sesuai dengan rencana strategis ANRI.
2. Memastikan integrasi ketentuan sistem manajemen keamanan informasi terdapat dalam proses bisnis ANRI.
3. Memastikan ketersediaan sumber daya yang dibutuhkan untuk sistem manajemen keamanan informasi.
4. Sistem manajemen keamanan informasi sesuai dengan tujuan ANRI.
5. Mengomunikasikan pentingnya sistem manajemen keamanan informasi yang efektif dan sesuai dengan ketentuan sistem manajemen keamanan informasi.
6. Mengarahkan dan memberikan dukungan terhadap tim sistem manajemen keamanan informasi dalam implementasi sistem manajemen keamanan informasi.
7. Mendorong perbaikan sistem manajemen keamanan informasi secara berkelanjutan.
8. Memastikan tersedianya regulasi untuk mendukung pelaksanaan sistem manajemen keamanan informasi.
9. Memastikan pengendalian terhadap risiko keamanan informasi yang bersifat internal dan eksternal terhadap implementasi sistem manajemen keamanan informasi.
10. Memastikan adanya komitmen untuk perbaikan yang berkelanjutan dari sistem manajemen keamanan informasi oleh seluruh pelaksana teknis keamanan sesuai kriteria audit.

B. Tim Sistem Manajemen Keamanan Informasi

Dalam rangka menunjang pelaksanaan sistem manajemen keamanan informasi, diperlukan organisasi yang dikelola secara profesional. Untuk mendukung hal tersebut harus adanya tugas dan tanggung jawab yang jelas dari setiap organisasi dalam penyelenggaraan fungsi keamanan informasi. Penetapan penanggung jawab merupakan kewenangan Kepala sebagai

pimpinan lembaga yang pelaksanaannya diserahkan kepada Pejabat Pimpinan Tinggi Madya yang mempunyai tugas dan fungsi di bidang kesekretariatan. Dalam melaksanakan tugas sebagai penanggung jawab, pejabat pimpinan tinggi madya dimaksud disebut sebagai Koordinator SPBE yang membentuk Tim Sistem Manajemen Keamanan Informasi. Tim Sistem Manajemen Keamanan Informasi ditetapkan oleh Pejabat Pimpinan Tinggi Madya di bidang kesekretariatan bertindak untuk dan atas nama Kepala. Tim Sistem Manajemen Keamanan Informasi memiliki tugas dan tanggung jawab meliputi:

1. Memastikan pelaksanaan kebijakan sistem manajemen keamanan informasi.
2. Mengendalikan dokumen sistem manajemen keamanan informasi untuk menjaga kemutakhiran dokumen dan efektivitas pelaksanaan operasional.
3. Melakukan pemetaan keperluan keamanan informasi.
4. Melakukan audit internal sistem manajemen keamanan informasi untuk memperbaiki penerapan sistem manajemen keamanan informasi dan menindaklanjuti temuan auditor.
5. Melakukan pemantauan dan evaluasi terhadap pelaksanaan sistem manajemen keamanan informasi di ANRI secara berkala untuk meningkatkan keamanan Informasi.
6. Mengidentifikasi dan mengkaji secara berkala persyaratan untuk menjaga kerahasiaan aset informasi yang dituangkan dalam dokumen kerahasiaan.
7. Menyampaikan laporan dan rekomendasi pelaksanaan sistem manajemen keamanan informasi.

Adapun Struktur Tim Sistem Manajemen Keamanan Informasi terdiri atas:

1. Komite Keamanan Informasi

Komite Keamanan Informasi yang dijabat oleh Pejabat Pimpinan Tinggi Madya yang mempunyai tugas dan fungsi di bidang kesekretariatan sebagai Ketua yang beranggotakan para Pimpinan Tinggi Madya, Komite Keamanan Informasi memiliki tugas dan tanggung jawab:

- a. Melakukan evaluasi pelaksanaan kebijakan keamanan informasi dan merekomendasikan pengendalian yang diperlukan.

- b. Melakukan koordinasi dalam perumusan dan penerapan kebijakan dan prosedur keamanan informasi.
 - c. Menyampaikan hasil evaluasi atas penerapan kebijakan keamanan informasi dan memberikan rekomendasi kepada Kepala untuk menjadi bahan pertimbangan dalam merumuskan kebijakan keamanan informasi sebagai bagian dari rencana strategis ANRI.
 - d. Memberikan rekomendasi efektivitas implementasi kebijakan keamanan informasi dan langkah mitigasi risiko.
 - e. Pengelolaan risiko keamanan informasi terutama untuk arsip digital perlu menerapkan proses manajemen risiko keamanan informasi secara berkala untuk mengidentifikasi, menilai, dan mengendalikan risiko yang terkait dengan keamanan arsip digital termasuk risiko akibat bencana alam, *human error*, *insider threat*, *ransomware*, dan kerusakan sistem.
 - f. Anggota komite keamanan informasi berlaku secara *ex officio*.
 - g. berkoordinasi dengan Tim Koordinasi SPBE/Pemerintah Digital dan forum tata kelola terkait untuk menyelaraskan kebijakan, program kerja, arsitektur, peta rencana, risiko, audit, dan evaluasi keamanan SPBE.
2. Pejabat Sistem Keamanan Informasi (*Chief Security Officer*)
- Pejabat Sistem Keamanan Informasi (*Chief Security Officer*) dijabat oleh Pejabat Pimpinan Tinggi Pratama yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi, Pejabat Sistem Manajemen Keamanan Informasi memiliki tugas dan tanggung jawab:
- a. Mengoordinasikan perumusan dan penyempurnaan kebijakan dan standar sistem manajemen keamanan informasi di lingkungan ANRI.
 - b. Menetapkan standar teknis dan prosedur keamanan aplikasi.
 - c. Memastikan seluruh pembangunan atau pengembangan aplikasi dan infrastruktur yang dilakukan oleh pihak ketiga memenuhi standar teknis dan prosedur keamanan informasi yang telah ditetapkan.
 - d. Memelihara dan mengendalikan penerapan kebijakan dan standar sistem manajemen keamanan informasi pada seluruh area di lingkungan ANRI yang menjadi tujuan

sasaran pengendalian.

- e. Menetapkan target keamanan informasi setiap tahunnya dan menyusun rencana kerja serta melakukan koordinasi dengan Pejabat Pengelola Informasi atas target dan rencana kerja yang ditetapkan.
- f. Memastikan efektivitas dan konsistensi penerapan kebijakan dan standar sistem manajemen keamanan informasi di lingkungan ANRI serta mengukur kinerja keseluruhan.
- g. Melaporkan kinerja penerapan kebijakan dan standar sistem manajemen keamanan informasi di lingkungan ANRI serta pencapaian target kepada Komite Keamanan Informasi.
- h. Menetapkan *Business Continuity Management* bersama Pejabat Pengelola Informasi sesuai arahan dari Komite Keamanan Informasi sebagai bentuk mitigasi risiko atas terjadinya insiden serta menjamin keberlangsungan operasional.
- i. Mengoordinasikan fungsi persandian dalam kerangka SMKI dan dilaksanakan oleh unit kerja sesuai tugas dan fungsi organisasi dengan melibatkan unit kerja terkait.

Dalam rangka pelaksanaan tugas dan tanggung jawab Pejabat Sistem Keamanan Informasi dibantu oleh Tim Pelaksana Sistem Manajemen Keamanan Informasi.

3. Pejabat Pengelola Informasi

Pejabat Pengelola Informasi dijabat oleh Pejabat Tinggi Pratama, Pejabat Pengelola Informasi memiliki tugas dan tanggung jawab:

- a. Memastikan pelaksanaan kebijakan dan prosedur keamanan informasi secara efektif pada unit kerja masing-masing.
- b. Memberikan arahan dan konsultasi atas penerapan kebijakan dan prosedur keamanan informasi pada unit kerja masing-masing.
- c. Melakukan sosialisasi dan pelatihan keamanan informasi pada unit kerja masing-masing.
- d. Menentukan jenis dan klasifikasi informasi pada unit kerja masing-masing sesuai ketentuan kebijakan keamanan informasi.
- e. Mengelola dan mengendalikan informasi pada unit kerja masing-masing.
- f. Melaporkan kinerja penerapan kebijakan dan standar sistem

manajemen keamanan informasi di lingkungan ANRI serta pencapaian target kepada Komite Keamanan Informasi.

4. Auditor Internal Keamanan Informasi

Auditor Internal Keamanan Informasi yang diketuai oleh Pejabat Pimpinan Tinggi Pratama yang melaksanakan tugas dan fungsi di bidang pengawasan internal di lingkungan ANRI. Auditor Internal Keamanan Informasi memiliki tugas dan tanggung jawab:

- a. Melakukan audit internal atas penerapan sistem manajemen keamanan informasi minimal 1 tahun sekali.
- b. Menyusun laporan hasil audit internal.
- c. Memverifikasi tindakan perbaikan dan pencegahan terhadap ketidaksesuaian yang ditemukan dalam proses audit internal.

Dalam rangka pelaksanaan tugas dan tanggung jawab Auditor Internal Keamanan Informasi dapat melibatkan pegawai dari unit kerja yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi dalam melaksanakan fungsi audit internal yang memiliki kompetensi audit dibuktikan dengan adanya sertifikat pelatihan audit TIK dan/atau audit keamanan informasi.

5. Tim Pelaksana Sistem Manajemen Keamanan Informasi

Tim Pelaksana Sistem Manajemen Keamanan Informasi yang beranggotakan pejabat fungsional pada *Chief Security Officer* (unit kerja yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi) memiliki tugas dan tanggung jawab:

- a. Menyusun, mengoordinasikan serta memantau pelaksanaan seluruh aktivitas dan proses sistem manajemen dalam rangka pemenuhan prasyarat sistem manajemen keamanan informasi.
- b. Mengoordinasikan pelaksanaan proses dan aktivitas sistem manajemen serta pengamanan informasi di organisasi.
- c. Mengoordinasikan proses peninjauan secara berkala terhadap implementasi sistem manajemen di organisasi.
- d. Memberikan laporan secara berkala terkait kondisi sistem manajemen keamanan informasi organisasi kepada penanggung jawab sistem manajemen.

- e. Dalam rangka mendukung perlindungan informasi strategis, informasi rahasia negara, informasi yang memerlukan pengamanan khusus, serta pemenuhan kematangan keamanan siber dan persandian, ANRI membentuk fungsi atau tim persandian sebagai bagian dari pelaksanaan Sistem Manajemen Keamanan Informasi.

Fungsi atau tim persandian sebagaimana dimaksud bertugas:

1. menyelenggarakan pengamanan informasi melalui penerapan kriptografi sesuai dengan ketentuan peraturan perundang-undangan;
2. mengelola sertifikat elektronik, layanan persandian, dan layanan pengamanan informasi lainnya;
3. mengelola kunci kriptografi yang digunakan dalam pengamanan sistem elektronik, komunikasi, pertukaran data, dan informasi strategis ANRI;
4. mengelola materiil sandi yang digunakan dalam pelaksanaan fungsi persandian, termasuk inventarisasi, penggunaan, penyimpanan, distribusi, pemeliharaan, pengamanan, evaluasi, dan pemusnahan sesuai dengan ketentuan peraturan perundang-undangan;
5. mengidentifikasi pola hubungan komunikasi sandi di lingkungan ANRI, baik antarunit kerja internal maupun dengan pihak eksternal yang berwenang;
6. melakukan analisis pola hubungan komunikasi sandi untuk menentukan kebutuhan pengamanan komunikasi, pertukaran informasi strategis, dan layanan persandian;
7. mengamankan komunikasi dan pertukaran informasi strategis yang memerlukan kerahasiaan, keutuhan, keaslian, dan kenirsangkalan;
8. memberikan rekomendasi penerapan pengamanan persandian pada Sistem Elektronik, Aplikasi, Infrastruktur Teknologi Informasi dan Komunikasi, serta proses bisnis ANRI;
9. menyusun dan/atau memberikan masukan terhadap kebijakan, prosedur, standar teknis, dan petunjuk teknis persandian;

10. melakukan koordinasi teknis persandian dengan Badan Siber dan Sandi Negara dan/atau pihak berwenang lainnya sesuai dengan ketentuan peraturan perundang-undangan; dan

11. menyusun laporan pelaksanaan fungsi persandian sebagai bagian dari evaluasi dan perbaikan berkelanjutan Sistem Manajemen Keamanan Informasi.

Pelaksanaan fungsi atau tim persandian dilakukan oleh unit kerja yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi dengan melibatkan unit kerja terkait sesuai dengan kebutuhan pengamanan informasi, komunikasi, dan layanan persandian.

BAB IV

PERENCANAAN

Untuk menjamin terwujudnya keamanan informasi di ANRI, perlu disusun Perencanaan sistem manajemen keamanan informasi oleh Tim Sistem Manajemen Keamanan Informasi Elektronik dan ditetapkan oleh Komite Keamanan Informasi.

Perencanaan tersebut dilakukan dengan merumuskan program kerja keamanan informasi dan target realisasi program kerja keamanan informasi yang wajib dilakukan setiap tahunnya sebagai dasar dilakukan evaluasi pada tahun berikutnya. Program kerja keamanan informasi terdiri dari edukasi kesadaran keamanan informasi, penilaian kerentanan keamanan informasi, peningkatan keamanan informasi, penanganan insiden, audit keamanan informasi. Perumusan program kerja manajemen keamanan berdasarkan kategori risiko keamanan yang ditentukan sesuai dengan hasil risk assessment atau ketentuan peraturan perundang-undangan. Selain program kerja, dalam rencana kerja juga dimuat target realisasi sesuai dengan kebutuhan unit kerja masing-masing. Penyusunan rencana kerja paling sedikit memuat:

A. Perencanaan edukasi kesadaran keamanan informasi dilaksanakan paling sedikit melalui kegiatan:

1. Sosialisasi.
2. Pelatihan.

Sosialisasi dan pelatihan mengenai keamanan informasi kepada seluruh pegawai ANRI dan pihak ketiga dilakukan secara berkala sesuai dengan tugas dan wewenang yang diberikan.

B. Perencanaan penilaian kerentanan keamanan informasi dilaksanakan paling sedikit melalui:

1. Menginventarisasi seluruh aset teknologi informasi dan komunikasi meliputi aplikasi, dan infrastruktur termasuk data dan informasi berdasarkan klasifikasi informasi.
2. Mengidentifikasi kerentanan dan ancaman terhadap aset teknologi dan informasi.
3. Mengukur tingkat risiko keamanan informasi.

C. Perencanaan peningkatan keamanan informasi dilaksanakan berdasarkan hasil dari penilaian kerentanan keamanan informasi. Perencanaan peningkatan keamanan informasi dilaksanakan paling sedikit melalui:

1. Menerapkan standar teknis dan prosedur keamanan informasi.
 2. Menguji fungsi keamanan terhadap aplikasi dan infrastruktur.
- D. Perencanaan penanganan insiden keamanan informasi dilaksanakan paling sedikit melalui:
1. Mengidentifikasi sumber serangan.
 2. Menganalisis informasi yang berkaitan dengan insiden selanjutnya.
 3. Memprioritaskan penanganan insiden berdasarkan tingkat dampak yang terjadi.
 4. Mendokumentasi bukti insiden yang terjadi.
 5. Memitigasi atau mengurangi dampak risiko keamanan informasi.
- E. Audit keamanan informasi dilakukan sesuai dengan ketentuan sebagai berikut:
1. Fungsi audit keamanan informasi dilaksanakan secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun sebagai bagian dari pelaksanaan audit internal atau dilaksanakan terpisah dari audit internal.
 2. Pelaksanaan fungsi audit internal dilakukan oleh unit kerja yang melaksanakan tugas dan fungsi di bidang pengawasan internal di lingkungan ANRI.
 3. Pelaksanaan fungsi audit internal dapat melibatkan pegawai dari unit kerja yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi.
 4. Dalam rangka pelaksanaan fungsi audit internal, wajib tersedia jejak audit (*audit trail*) terhadap seluruh kegiatan penyelenggaraan teknologi informasi untuk keperluan pengawasan, penegakan hukum, penyelesaian sengketa, verifikasi, pengujian, dan pemeriksaan lainnya.
 5. Pelaksanaan fungsi audit internal dapat dilakukan oleh auditor eksternal dalam hal belum tersedianya tenaga yang memiliki kompetensi.
 6. Pelaksanaan audit keamanan SPBE internal dilaksanakan sebelum audit keamanan SPBE eksternal oleh LATIK Pemerintah atau LATIK Terakreditasi yang terdaftar.
 7. Penyusunan audit keamanan internal dilakukan berdasarkan perencanaan audit keamanan SPBE yang paling sedikit mempertimbangkan:
 - a. Aplikasi SPBE dan/atau Infrastruktur SPBE yang dimiliki,

- dikelola, dan/atau digunakan oleh ANRI;
 - b. Risiko pada Aplikasi SPBE dan/atau Infrastruktur SPBE;
 - c. Kategori Sistem Elektronik;
 - d. Tingkat vitalitas Sistem Elektronik; dan/atau
 - e. Hasil audit keamanan Aplikasi SPBE dan/atau Infrastruktur SPBE sebelumnya
8. Setiap temuan audit harus dicatat dan ditindaklanjuti melalui rencana aksi yang paling sedikit memuat akar masalah, tingkat risiko, tindakan perbaikan, penanggung jawab, target penyelesaian, status, bukti dukung, dan verifikasi efektivitas penyelesaian.
- F. Perencanaan penyusunan dan pemutakhiran dokumen turunan Sistem Manajemen Keamanan Informasi.
- Dalam rangka memastikan pelaksanaan Sistem Manajemen Keamanan Informasi berjalan efektif, terukur, terdokumentasi, dan sesuai dengan ketentuan peraturan perundang-undangan, ANRI menyusun dan menetapkan dokumen turunan Sistem Manajemen Keamanan Informasi dalam bentuk pedoman, prosedur, standar teknis, petunjuk teknis, dan/atau dokumen operasional lainnya. Dokumen turunan sebagaimana dimaksud paling sedikit mencakup:
- a. prosedur penanganan insiden keamanan informasi;
 - b. skenario atau playbook penanganan insiden keamanan informasi;
 - c. prosedur pelaksanaan simulasi insiden keamanan informasi;
 - d. prosedur perlindungan data pribadi dan pemenuhan hak subjek data pribadi;
 - e. prosedur Secure Software Development Life Cycle dalam pengembangan, perubahan, dan pemeliharaan aplikasi;
 - f. prosedur Vulnerability Assessment terhadap aplikasi dan/atau infrastruktur teknologi informasi dan komunikasi;
 - g. prosedur uji penetrasi aplikasi dan/atau infrastruktur teknologi informasi dan komunikasi;
 - h. prosedur penggunaan perangkat pribadi untuk mengakses layanan ANRI atau Bring Your Own Device;
 - i. prosedur evaluasi kepatuhan Sistem Manajemen Keamanan Informasi; dan
 - j. petunjuk teknis penggunaan kriptografi dan pengamanan file, termasuk pengamanan informasi pada layanan komputasi awan.

Penyusunan, penetapan, penerapan, evaluasi, dan pemutakhiran dokumen turunan sebagaimana dimaksud dilaksanakan oleh unit kerja yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi bersama unit kerja terkait sesuai dengan tugas dan kewenangannya. Dokumen turunan tersebut dilakukan revidi secara berkala dan/atau sewaktu-waktu apabila terdapat perubahan regulasi, perubahan risiko, hasil audit, hasil evaluasi, insiden keamanan informasi, atau perkembangan teknologi informasi dan komunikasi.

Selain itu, dalam perencanaan diperlukan pengelolaan keberlanjutan keamanan informasi. Pengelolaan keberlangsungan kegiatan dilaksanakan dengan cara kombinasi pengendalian pencegahan dan pemulihan (*recovery*). Pengelolaan keberlanjutan keamanan informasi dalam pengelolaan keberlangsungan kegiatan mencakup hal-hal sebagai berikut:

A. Perencanaan Keberlanjutan Keamanan Informasi

1. Penentuan dan pengintegrasian prasyarat keberlanjutan keamanan informasi dengan prasyarat keberlanjutan kegiatan ANRI.
2. Prasyarat keberlanjutan keamanan informasi mencakup teknik, metode atau infrastruktur yang diperlukan untuk menjamin keberlanjutan keamanan informasi di ANRI pada saat dan setelah terjadinya gangguan besar atau bencana.
3. Penetapan, pendokumentasian, implementasi dan pemeliharaan proses, prosedur dan kontrol yang diperlukan untuk menjamin keberlanjutan keamanan informasi sesuai prasyarat yang telah ditetapkan pada saat dan setelah terjadinya gangguan besar atau bencana.
4. Verifikasi keberlanjutan kontrol keamanan informasi yang telah ditetapkan dan diimplementasikan secara berkala untuk menjamin kesesuaian dan efektivitasnya pada saat dan setelah terjadinya gangguan besar atau bencana.
5. Prasyarat keamanan informasi dapat diintegrasikan pada siklus proses *business continuity management* yang mencakup:
 - a. Pemahaman kebutuhan ANRI.
 - b. Penentuan strategi BCM (*Business Continuity Management*).
 - c. Pengembangan dan implementasi

rencana penanggulangan/keberlanjutan kegiatan.

- d. Pengujian, pemeliharaan dan peninjauan rencana penanggulangan/keberlanjutan kegiatan.

B. Penerapan Keberlanjutan Keamanan Informasi

1. Proses *business continuity management* dikembangkan dan dipelihara dengan mempertimbangkan kebutuhan keamanan informasi untuk keberlangsungan kegiatan ANRI dengan mempertimbangkan:
 - a. Pemahaman terhadap berbagai risiko yang dihadapi ANRI terhadap insiden pada operasional atau keadaan darurat yang disebabkan oleh bencana alam yang mencakup prioritasasi proses layanan yang kritis.
 - b. Identifikasi dari seluruh aset yang digunakan oleh proses layanan kritikal.
 - c. Pengembangan dan dokumentasi perencanaan keberlangsungan kegiatan (*Bussiness Continuity Plan/BCP*) yang mencakup strategi keberlangsungan kegiatan.
 - d. Pengalokasian tugas dan tanggung jawab proses keberlangsungan kegiatan dalam proses dan struktur ANRI.
2. Penetapan tim penanggulangan dan pemulihan bencana dan menetapkan koordinasi pemulihan BCP dalam kerangka kerja BCP.
3. Proses perencanaan keberlanjutan keamanan informasi harus berfokus pada prasyarat keamanan informasi ANRI.
4. Rencana keberlanjutan keamanan informasi perlu mempertimbangkan kerentanan (*vulnerability*) ANRI termasuk dalam hal tersebut adalah informasi sensitif yang dimiliki. Hal ini diperlukan untuk merencanakan tindakan guna memastikan kerentanan tersebut dapat dikendalikan dan dikelola dengan baik.
5. Setiap proses atau rencana keberlanjutan keamanan informasi, seperti prosedur darurat atau rencana manual untuk *fallback*, harus memiliki pemilik proses (*process owner*) yang khusus dan bertanggung jawab untuk mengelola proses atau rencana tersebut. Hal ini termasuk proses atau rencana yang melibatkan penyedia jasa pihak

ketiga.

6. ANRI harus menilai risiko yang berkaitan kritikalitas proses yang dijalankan terkait dengan *business continuity* sebagai kajian mengenai *Business Impact Analysis* (BIA) dengan mengidentifikasi dampak kegagalan maupun gangguan terhadap proses bisnis.

C. Pengujian *Continuity Plan* yang Mencakup Aspek Keamanan Informasi

1. Penanggung jawab sistem di ANRI harus melakukan koordinasi terkait dengan perencanaan *business continuity* dalam rangka memelihara dan memastikan proses pemulihan operasi sistem informasi pada saat terjadi gangguan pada proses bisnis yang kritikal.
2. Proses perencanaan dan pengembangan *Business Continuity Plan* meliputi:
 - a. Identifikasi dan kesepakatan untuk semua tanggung jawab pada tim BCP di ANRI yang terlibat dalam pemulihan proses darurat.
 - b. Penyediaan prosedur operasional bisnis pada proses *recovery* dan *restoration*.
 - c. Rencana pelatihan untuk pegawai yang terlibat dalam proses- proses dalam *Business Continuity Plan*.
 - d. Pengujian *Business Continuity Plan*.
3. ANRI harus memastikan dokumen BCP tersimpan dan selalu *up- to-date*.
4. Pengujian rencana keberlanjutan keamanan informasi secara reguler perlu dilakukan untuk memastikan bahwa seluruh anggota dari tim pemulihan (*recovery*) serta pegawai lain yang berhubungan dengan tim pemulihan memahami tugas dan tanggung jawabnya dalam rencana keberlanjutan keamanan informasi terutama yang terkait dengan aspek keamanan informasi.
5. Penetapan rencana atau skenario pengujian yang berisi bagaimana dan dalam frekuensi apa setiap elemen rencana keberlanjutan keamanan informasi akan diuji.
6. Guna menjamin rencana keberlanjutan keamanan informasi agar dapat berjalan dalam kondisi nyata, beberapa cara berikut harus dilaksanakan:

- a. Pengujian melalui simulasi di atas kertas (*table-top testing*) atas skenario yang ada pada rencana keberlanjutan keamanan informasi, simulasi di atas kertas ini dapat dilakukan melalui diskusi bersama mengenai langkah-langkah yang perlu dilakukan apabila terjadi gangguan terhadap operasional bisnis.
- b. Simulasi nyata, terutama untuk melatih personel yang terlibat dalam rencana keberlanjutan keamanan informasi agar tugas dan tanggung jawab masing-masing personel dalam kondisi gangguan dapat dipahami dengan baik.
- c. Pengujian pemulihan sistem secara teknis untuk memastikan bahwa sistem informasi ANRI dapat di-*restore* dengan baik.
- d. Ketentuan pemulihan arsip digital dalam keadaan darurat harus disusun dan diuji secara berkala. Rencana pemulihan arsip digital (*Disaster Recovery Plan*) untuk memastikan kelangsungan layanan informasi kearsipan dan pemulihan data apabila terjadi bencana atau serangan siber.
- e. Pengujian pemulihan (*recovery*) menggunakan fasilitas pada lokasi alternatif. Hal ini dilakukan dengan menjalankan proses kegiatan pada lokasi utama secara paralel dengan proses kegiatan pada fasilitas *recover* pada lokasi alternatif.
- f. Pengujian fasilitas dan layanan yang disediakan oleh pihak ketiga untuk menjamin layanan yang disediakan oleh supplier eksternal sesuai dengan perjanjian dalam kontrak kerja.
- g. Pengujian secara menyeluruh dengan melibatkan seluruh komponen ANRI termasuk pegawai, peralatan, fasilitas serta proses kegiatan ANRI untuk menjamin kesiapan seluruh komponen ANRI dalam menghadapi gangguan bisnis.
- h. Pendokumentasian hasil pengujian rencana keberlanjutan keamanan informasi secara komprehensif untuk kemudian ditinjau guna menemukan tindakan-tindakan perbaikan yang dapat diambil dalam rangka

penyempurnaan rencana keberlanjutan keamanan informasi.

7. Peninjauan rencana keberlanjutan keamanan informasi dilakukan secara berkala untuk menjamin rencana yang ada tetap sesuai dengan perubahan dan/atau perkembangan layanan ANRI.
8. Perubahan pada rencana keberlanjutan keamanan informasi dilakukan secara formal dan kemudian didistribusikan kepada seluruh komponen dalam ANRI.
9. Perubahan dan/atau perkembangan layanan yang dapat menjadi bahan pertimbangan perubahan rencana keberlanjutan keamanan informasi antara lain pembelian perangkat baru, *upgrade* sistem serta perubahan pada:
 - a. Personel.
 - b. Alamat, lokasi, fasilitas dan sumber daya kerja.
 - c. Kontrol keamanan informasi.

10. Penanggung Jawab Pengelolaan Keberlanjutan Keamanan Informasi

Penanggung jawab pengelolaan keberlanjutan keamanan informasi adalah unit kerja yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi.

DUKUNGAN PENGOPERASIAN

Dalam mendukung pelaksanaan Sistem Manajemen Keamanan Informasi, diperlukan dukungan pengoperasian untuk meningkatkan kapasitas terhadap:

A. Sumber Daya Manusia Keamanan Informasi

Sumber daya manusia mencakup semua pihak yang terlibat dalam proses keamanan informasi termasuk tugas pokok dan fungsinya. Sumber daya manusia keamanan informasi paling sedikit memiliki kompetensi keamanan infrastruktur teknologi informasi dan komunikasi serta keamanan aplikasi. Untuk memenuhi kompetensi paling sedikit didukung dengan kegiatan pelatihan dan/atau sertifikasi kompetensi keamanan infrastruktur teknologi dan keamanan aplikasi serta bimbingan teknis mengenai standar keamanan SPBE. Dalam hal pelatihan dan sertifikasi audit keamanan SPBE harus diselenggarakan oleh BSSN atau lembaga pelatihan lain yang mendapat pengakuan dari BSSN.

Dalam rangka memastikan kecukupan kuantitas dan kualitas sumber daya manusia keamanan informasi, ANRI melaksanakan analisis kesenjangan kompetensi sumber daya manusia keamanan siber dan persandian secara berkala. Analisis kesenjangan kompetensi sebagaimana dimaksud dilakukan untuk mengidentifikasi kebutuhan kompetensi, ketersediaan kompetensi, tingkat kecukupan personel, kebutuhan pelatihan, kebutuhan sertifikasi, serta prioritas pengembangan kapasitas sumber daya manusia keamanan informasi.

Analisis kesenjangan kompetensi sumber daya manusia keamanan siber dan persandian paling sedikit mempertimbangkan tugas dan fungsi jabatan, peran dalam Sistem Manajemen Keamanan Informasi, kebutuhan pengamanan aplikasi dan infrastruktur teknologi informasi dan komunikasi, kebutuhan audit keamanan informasi, kebutuhan penanganan insiden, kebutuhan pengelolaan keamanan siber dan persandian, hasil audit, hasil evaluasi, hasil pengukuran tingkat kematangan keamanan siber dan persandian, serta perkembangan risiko dan ancaman keamanan siber.

Hasil analisis kesenjangan kompetensi digunakan sebagai dasar penyusunan program pengembangan kompetensi secara berkala,

yang dapat dilaksanakan melalui pelatihan, bimbingan teknis, sertifikasi, workshop, simulasi, knowledge sharing, latihan penanganan insiden, dan/atau bentuk pengembangan kompetensi lainnya sesuai dengan ketentuan Standar Kompetensi Kerja Nasional Indonesia (SKKNI) Keamanan Informasi. Program pengembangan kompetensi disusun untuk mendukung pemenuhan kebutuhan kompetensi keamanan infrastruktur teknologi informasi dan komunikasi, keamanan aplikasi, audit keamanan informasi, pengelolaan risiko, perlindungan data pribadi, pengelolaan insiden, pengelolaan log dan pemantauan keamanan, serta persandian.

Pelaksanaan program pengembangan kompetensi sumber daya manusia keamanan informasi dilakukan secara rutin, terdokumentasi, dievaluasi, dan dimutakhirkan sesuai dengan kebutuhan organisasi, perubahan regulasi, hasil audit, hasil evaluasi, perkembangan teknologi, serta perkembangan ancaman keamanan siber.

Penanggung jawab pelaksanaan analisis kesenjangan kompetensi dan program pengembangan kompetensi sumber daya manusia keamanan informasi adalah unit kerja yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi bersama unit kerja yang melaksanakan tugas dan fungsi di bidang sumber daya manusia/kepegawaian serta unit kerja terkait sesuai dengan kewenangannya.

Pada pengelolaan sumber daya manusia dilakukan sebelum status kepegawaian dimulai dan selama status kepegawaian berjalan.

1. Sebelum Status Kepegawaian Dimulai

Pengaturan pengelolaan keamanan sumber daya manusia sebelum status kepegawaian dimulai mencakup:

a. Pemeriksaan (*Screening*)

- 1) Pemeriksaan (*screening*) dan verifikasi atas latar belakang masing masing calon pegawai atau pihak eksternal sebelum bekerja.
- 2) Penerimaan pegawai di lingkungan ANRI harus sesuai dengan ketentuan yang berlaku.

b. Syarat dan Ketentuan Pegawai

- 1) Setiap pegawai dan pihak eksternal di lingkungan ANRI bertanggung jawab untuk menjaga keamanan informasi ANRI.

- 2) Setiap pengguna informasi maupun sistem informasi ANRI harus menyetujui dan menandatangani syarat dan ketentuan terkait dengan keamanan informasi dan sistem informasi ANRI.
- 3) Pegawai kontrak wajib menandatangani Perjanjian Kerahasiaan terkait keamanan informasi dan kepatuhan.
- 4) Sumber daya manusia yang terkait langsung dengan sistem manajemen keamanan informasi paling sedikit harus memiliki kompetensi:
 - a) Keamanan infrastruktur teknologi informasi dan komunikasi.
 - b) Keamanan aplikasi.
- 5) Standar kompetensi pegawai dibuktikan setidaknya dengan:
 - a) Telah mengikuti pelatihan dan/atau sertifikasi kompetensi keamanan infrastruktur teknologi informasi dan komunikasi dan keamanan aplikasi.
 - b) Telah mengikuti bimbingan teknis mengenai standar keamanan informasi.

2. Selama Status Kepegawaian Berjalan.

Pengaturan pengelolaan keamanan sumber daya manusia selama status kepegawaian berjalan mencakup:

a. Tanggung Jawab Pengawasan Kepatuhan

- 1) Seluruh pejabat struktural wajib mengawasi kepatuhan pegawai terhadap sistem manajemen keamanan informasi di lingkungan ANRI.
- 2) Seluruh pejabat struktural bertanggung jawab memastikan bahwa seluruh pengguna informasi dan sistem informasi:
 - a) Memahami dan menerapkan tugas dan tanggung jawabnya dalam sistem keamanan informasi ANRI;
 - b) Mematuhi seluruh tugas dan tanggung jawabnya sesuai dengan syarat dan ketentuan pada perjanjian kerja dan kebijakan keamanan informasi ANRI;
 - c) Memiliki keahlian dan kualifikasi keamanan informasi sesuai dengan tugas dan tanggung jawabnya.

b. Penanaman Kesadaran Terkait Keamanan Informasi

- 1) Sosialisasi dan pelatihan mengenai keamanan informasi kepada seluruh pegawai ANRI dan pihak ketiga dilakukan secara berkala sesuai dengan tugas dan wewenang yang diberikan.
- 2) Sosialisasi dan pelatihan mengenai keamanan informasi dilaksanakan oleh unit kerja yang memiliki tugas melaksanakan urusan kepegawaian.

c. Proses Pendisiplinan

Proses penerapan kedisiplinan disesuaikan dengan :

- 1) Kebijakan pendisiplinan pegawai terkait pelanggaran ketentuan keamanan informasi disusun oleh unit kerja yang memiliki tugas melaksanakan urusan kepegawaian.
- 2) Penerapan proses pendisiplinan secara formal sesuai dengan aturan yang berlaku di ANRI bagi setiap pegawai yang melakukan pelanggaran terkait keamanan informasi.
- 3) Proses pendisiplinan atas pelanggaran keamanan informasi dilaksanakan oleh unit kerja yang memiliki tugas melaksanakan urusan kepegawaian.

d. Pemberhentian atau Pergantian Status Pegawai

Pemberhentian atau pergantian status pegawai harus mempertimbangkan hal hal sebagai berikut:

- 1) Dalam hal terjadi proses perubahan atau pemberhentian (terminasi) hubungan kerja maka dilakukan langkah-langkah untuk melindungi kepentingan ANRI dengan mendefinisikan, mengomunikasikan dan memberlakukan tanggung jawab dan tugas keamanan informasi kepada pegawai dan pihak eksternal.
- 2) Tanggung jawab pegawai pada saat dan setelah proses pemberhentian atau pergantian status kepegawaian harus dikomunikasikan dengan jelas kepada personel yang bersangkutan.

Adapun beberapa hal terkait sumber daya manusia keamanan informasi yang perlu diperhatikan, diantaranya:

1. Setiap pemilik informasi maupun pengguna sistem informasi ANRI harus menyetujui dan menandatangani syarat dan ketentuan terkait dengan keamanan informasi

dan sistem informasi ANRI.

2. Setiap pegawai kontrak di lingkungan ANRI wajib menandatangani perjanjian kerahasiaan terkait keamanan informasi.
3. Dalam hal terdapat perubahan dan/atau pemberhentian pegawai maka wajib dilakukan langkah-langkah untuk melindungi kepentingan ANRI sesuai dengan prosedur yang berlaku.
4. Pegawai ANRI yang melanggar ketentuan dan/atau kebijakan keamanan informasi mendapatkan sanksi sesuai dengan ketentuan peraturan perundang-undangan.

B. Anggaran Keamanan Informasi

Anggaran keamanan informasi disusun berdasarkan perencanaan yang telah ditetapkan sesuai ketentuan peraturan perundang-undangan.

BAB VI

EVALUASI KINERJA

Untuk memastikan pelaksanaan sistem manajemen keamanan informasi terlaksana sesuai dengan ketentuan yang berlaku, maka perlu dilakukan pelaksanaan Evaluasi sistem manajemen keamanan informasi dengan memperhatikan hal-hal berikut:

- A. Evaluasi terhadap sistem manajemen keamanan informasi dilakukan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.
- B. Komite Keamanan Informasi bertanggung jawab memberi arahan dan keputusan untuk melakukan perbaikan atau penyempurnaan (*improvement*) terhadap sistem manajemen keamanan informasi.
- C. Evaluasi sistem manajemen keamanan informasi dilaksanakan dengan:
 - 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. Menganalisis efektivitas pelaksanaan keamanan informasi.
 - 5. Mendukung dan merealisasikan program audit keamanan informasi.
 - 6. Menilai tingkat kepatuhan terhadap peraturan perundang-undangan maupun standar keamanan informasi yang berlaku.
- D. Pejabat Sistem Keamanan Informasi dan Pejabat Pengelola Informasi bertanggung jawab untuk merangkum hasil pemantauan dan pengukuran efektivitas penerapan sistem manajemen keamanan informasi pada masing-masing unit kerja, menganalisis dan merekomendasikan penyempurnaan terkait aspek-aspek, antara lain:
 - 1. Sasaran dan pencapaiannya.
 - 2. Risiko dan rencana mitigasi.
 - 3. Insiden dan penyelesaiannya.
 - 4. Hasil audit dan tindak lanjut audit.
- E. Pejabat Sistem Keamanan Informasi dan Pejabat Pengelola Informasi melaporkan hasil pemantauan dan pengukuran efektivitas penerapan Sistem Manajemen Keamanan Informasi kepada Komite Keamanan Informasi.
- F. Internal Audit memberikan laporan hasil audit teknologi informasi dan komunikasi secara berkala sesuai dengan jadwal audit yang

telah ditentukan kepada Komite Keamanan Informasi.

- G. Komite Keamanan Informasi melakukan evaluasi terhadap pelaksanaan sistem manajemen keamanan informasi berdasarkan hasil pemeriksaan audit, hasil pemantauan dan pengendalian risiko keamanan informasi dan tingkat kepatuhan, serta hasil pemantauan dan pengukuran efektivitas penerapan sistem manajemen keamanan informasi di masing-masing unit kerja untuk dilakukan analisa terhadap pelaksanaan kebijakan sistem manajemen keamanan informasi.
- H. Proses Pengendalian Terhadap Audit Sistem Informasi, mencakup hal-hal:
1. Kebutuhan audit dan aktivitas yang melibatkan pemeriksaan sistem operasional harus direncanakan dan disetujui pejabat yang berwenang untuk meminimalkan risiko gangguan pada proses bisnis.
 2. Auditor sistem informasi perlu merencanakan kebutuhan audit yang melibatkan pemeriksaan sistem operasional yang meliputi:
 - a. Ruang lingkup dari pemeriksaan audit harus disepakati dan dikendalikan.
 - b. Seluruh akses ke sistem informasi harus dimonitor dan dicatat dalam log untuk menghasilkan *reference trail*.
 - c. Pelaksana audit harus bersifat independen dari aktivitas yang diaudit.
 - d. Audit *requirements* perlu disetujui dengan pihak yang berwenang.
 - e. Hak Akses terhadap data dan aplikasi dalam proses audit perlu dibatasi hanya dengan akses *read only*.
 - f. Hak akses selain *read only* hanya dibolehkan untuk salinan (*copy*) dari *system files*. Salinan (*copy*) tersebut perlu segera dihapus setelah proses audit selesai atau diberikan perlindungan yang sesuai apabila ada kebutuhan untuk dokumentasi.
 - g. Sumber daya yang dibutuhkan untuk melakukan audit harus diidentifikasi dan disediakan.
 - h. Proses audit test pada sistem informasi dilakukan di luar jam operasional ANRI.
 - i. Seluruh prosedur, *requirements* dan tanggung jawab dalam

proses audit sistem informasi harus didokumentasi.

3. Penanggung Jawab Pengendalian Audit Sistem Informasi
Penanggung jawab pengendalian audit sistem informasi adalah unit kerja yang melaksanakan tugas dan fungsi di bidang pengawasan internal di lingkungan ANRI dengan melibatkan unit kerja yang melaksanakan tugas dan fungsi di bidang teknologi informasi dan komunikasi.
- I. Komite Keamanan Informasi memberikan laporan pelaksanaan sistem manajemen keamanan informasi kepada Kepala sebagai bahan pertimbangan untuk kebijakan ANRI selanjutnya apabila diperlukan.

BAB VII

PERBAIKAN BERKELANJUTAN

Sebagai bentuk tindak lanjut atas pelaksanaan evaluasi sistem manajemen keamanan informasi, maka diperlukan langkah-langkah tertentu untuk melakukan perbaikan terhadap sistem manajemen keamanan informasi. Perbaikan sistem manajemen keamanan informasi dilakukan oleh Pejabat Sistem Keamanan Informasi. Adapun langkah perbaikan sistem manajemen keamanan informasi dilakukan dengan cara:

- A. Mengatasi permasalahan dalam pelaksanaan keamanan informasi, meliputi:
 1. Memperbaiki atau mengubah kebijakan yang ada untuk disesuaikan dengan kebutuhan dan/atau perkembangan teknologi informasi dan komunikasi.
 2. Memperbaiki atau mengubah sistem teknologi informasi dan komunikasi ANRI.
 3. Tindakan lainnya yang dianggap perlu berdasarkan hasil evaluasi ANRI,
- B. Memperbaiki pelaksanaan keamanan informasi secara periodik.
 1. Melakukan tindak lanjut atas hasil temuan audit.
 2. Melakukan peningkatan kesadaran (*awareness*) atas keamanan informasi terhadap pegawai ANRI atau pihak terkait lainnya.
 3. Melakukan perbaikan terhadap klasifikasi dan identifikasi risiko serta proses pengendalian risiko.
 4. Tindakan lainnya yang dianggap perlu berdasarkan hasil evaluasi ANRI.
- C. Perbaikan berkelanjutan dilakukan melalui pencatatan ketidaksesuaian, analisis akar masalah, penetapan tindakan korektif dan tindakan pencegahan, penanggung jawab, target penyelesaian, pemantauan, dokumentasi bukti, serta verifikasi efektivitas tindakan.

BAB VIII
PENUTUP

Keputusan ini disusun sebagai acuan bagi seluruh pegawai dan unit kerja dalam pelaksanaan sistem manajemen keamanan informasi di lingkungan ANRI untuk melindungi kerahasiaan, integritas, dan ketersediaan aset informasi dari berbagai bentuk ancaman keamanan informasi baik dari dalam maupun luar lingkungan Arsip Nasional Republik Indonesia.

KEPALA ARSIP NASIONAL REPUBLIK INDONESIA,



MEGO PINANDITO