BADAN KEPEGAWAIAN NEGARA

KEPUTUSAN KEPALA BADAN KEPEGAWAIAN NEGARA
NOMOR 209 TAHUN 2024
TENTANG
TATA KELOLA KEAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN KEPEGAWAIAN NEGARA,

Menimbang : a. bahwa untuk menjamin kerahasiaan (*confidentiality*), ketersediaan (*availability*), keutuhan (*integrity*) aset informasi dan keandalan (*reliability*) infrastruktur Teknologi Informasi dan Komunikasi (TIK), perlu dilakukan tata kelola keamanan informasi di lingkungan Badan Kepegawaian Negara;

b. bahwa guna meningkatkan efektivitas dan efisiensi pengelolaan keamanan informasi sesuai Standar Nasional Indonesia (SNI) ISO/IEC 27001:2022, perlu mengatur ketentuan mengenai tata kelola keamanan informasi yang meliputi sistem manajemen keamanan informasi, penggunaan akun dan kata sandi, surat elektronik, internet, dan penerapan sertifikat elektronik di lingkungan Badan Kepegawaian Negara;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Keputusan Kepala Badan Kepegawaian Negara tentang Tata Kelola Keamanan Informasi;

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);

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 20 Tahun 2023 tentang Aparatur Sipil Negara (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 141, Tambahan Lembaran Negara Republik Indonesia Nomor 6897);
5. Peraturan Presiden Nomor 58 Tahun 2013 tentang Badan Kepegawaian Negara (Lembaran Negara Republik Indonesia Tahun 2013 Nomor 128);
6. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
7. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112);
8. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);
9. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2016 Nomor 1829);
10. Peraturan Menteri Pendayagunaan Aparatur Negara Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 994);

11. Peraturan Badan Kepegawaian Negara Nomor 29 Tahun 2020 tentang Organisasi dan Tata Kerja Badan Kepegawaian Negara (Berita Negara Republik Indonesia Tahun 2020 Nomor 1728);
12. Peraturan Badan Kepegawaian Negara Nomor 31 Tahun 2020 tentang Organisasi dan Tata Kerja Kantor Regional Badan Kepegawaian Negara (Berita Negara Republik Indonesia Tahun 2020 Nomor 1730);
13. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375);
14. 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 2020 Nomor 541);
15. Keputusan Kepala Badan Kepegawaian Negara Nomor 249.1/KEP/2020 tentang Pedoman Tata Kelola Teknologi Informasi dan Komunikasi di Lingkungan Badan Kepegawaian Negara;
16. Keputusan Kepala Badan Kepegawaian Negara Nomor 83.2 Tahun 2021 tentang Pedoman Penyelenggaraan Manajemen Risiko di Lingkungan Badan Kepegawaian Negara;
17. Keputusan Kepala Badan Kepegawaian Negara Nomor 350.8 Tahun 2023 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Badan Kepegawaian Negara;

MEMUTUSKAN:

Menetapkan : KEPUTUSAN KEPALA BADAN KEPEGAWAIAN NEGARA TENTANG TATA KELOLA KEAMANAN INFORMASI.

KESATU : Menetapkan Tata Kelola Keamanan Informasi sebagaimana tercantum dalam Lampiran yang merupakan bagian yang tidak terpisahkan dari Keputusan ini.

KEDUA : Dengan ditetapkannya Keputusan ini, maka Keputusan Kepala Badan Kepegawaian Negara Nomor 161.8 Tahun 2022 tentang Tata Kelola Infrastruktur Teknologi Informasi Komunikasi dan Tata Kelola Keamanan Informasi, dicabut dan dinyatakan tidak berlaku.

KETIGA : Keputusan ini berlaku sejak tanggal ditetapkan dengan ketentuan apabila dikemudian hari terdapat kekeliruan akan diperbaiki sebagaimana mestinya.

Ditetapkan di Jakarta
pada tanggal 10 Juni 2024

Plt. KEPALA
BADAN KEPEGAWAIAN NEGARA,

Ditandatangani Secara Elektronik
HARYOMO DWI PUTRANTO

LAMPIRAN
KEPUTUSAN KEPALA BADAN KEPEGAWAIAN NEGARA
NOMOR : 209 TAHUN 2024
TANGGAL : 10 JUNI 2024

TATA KELOLA KEAMANAN INFORMASI

A. KETENTUAN UMUM

Dalam Keputusan ini yang dimaksud dengan:

1. Tata Kelola Keamanan Informasi adalah pembentukan dan pemeliharaan lingkungan pengendalian risiko yang berkaitan dengan kerahasiaan, integritas, dan ketersediaan informasi dan proses pendukungnya dan sistem.
2. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan TIK untuk memberikan layanan kepada pengguna SPBE.
3. Pusat Data (*Data Center)* Badan Kepegawaian Negara yang selanjutnya disebut Pusat Data/DC BKN adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, serta pemulihan data yang berada di bawah pengelolaan Badan Kepegawaian Negara.
4. Badan Kepegawaian Negara yang selanjutnya disingkat BKN adalah lembaga yang melaksanakan tugas dan fungsi pemerintahan di bidang perumusan dan penetapan kebijakan teknis, pembinaan, penyelenggaraan pelayanan, dan pengendalian atas pelaksanaan kebijakan teknis Manajemen ASN.

B. MAKSUD DAN TUJUAN

Keputusan ini dimaksudkan sebagai pedoman dalam melindungi aset informasi Badan Kepegawaian Negara dari berbagai bentuk ancaman baik dari dalam maupun luar lingkungan Badan Kepegawaian Negara.

Keputusan ini bertujuan untuk menjamin ketersediaan (*availability*), keutuhan (*integrity*), dan kerahasiaan (*confidentiality*) aset informasi, keaslian (*authentication*), dan kenirsangkalan (*non-repudiation*) aset informasi selalu terjaga dan terpelihara dengan baik.

C. RUANG LINGKUP

Keputusan ini mengatur ruang lingkup Tata Kelola Keamanan Informasi yang terdiri atas:

a. Pengendalian Umum;
b. Pengendalian Pengelolaan Aset Informasi;
c. Pengendalian Organisasi Keamanan Informasi;
d. Pengendalian Keamanan Sumber Daya Manusia;
e. Pengendalian Keamanan Fisik dan Lingkungan;
f. Pengendalian Pengelolaan Komunikasi dan Operasional;
g. Pengendalian Akses;
h. Pengendalian Keamanan Informasi Dalam Pengadaan, Pengembangan, dan Pemeliharaan Sistem Informasi;
i. Pengendalian Pengelolaan Gangguan Keamanan Informasi.
j. Pengendalian Keamanan Informasi Dalam Pengelolaan Kelangsungan Kegiatan; dan
k. Pengendalian Kepatuhan.

D. PENGENDALIAN UMUM

1. TUJUAN

Tata Kelola Keamanan Informasi ini digunakan sebagai pedoman dalam melindungi aset informasi Badan Kepegawaian Negara dari berbagai bentuk ancaman baik dari dalam maupun luar lingkungan Badan Kepegawaian Negara.

Pengamanan dan perlindungan ini dilakukan dalam rangka menjamin ketersediaan (*availability*), keutuhan (*integrity*), dan kerahasiaan (*confidentiality*) aset informasi, keaslian (*authentication*), dan kenirsangkalan (*non-repudiation*) aset informasi selalu terjaga dan terpelihara dengan baik.

2. RUANG LINGKUP

a. Kebijakan dan standar ini berlaku untuk pengelolaan keamanan seluruh aset informasi Badan Kepegawaian Negara dan dilaksanakan oleh seluruh unit kerja dan/atau pegawai Badan Kepegawaian Negara baik sebagai pengguna maupun pengelola Teknologi Informasi dan Komunikasi (TIK), dan pihak ketiga di lingkungan BKN.

b. Aset informasi BKN merupakan aset dalam bentuk:
   1) Data/dokumen, meliputi: data kepegawaian atau data lain yang terkait dengan data pribadi pegawai sebagaimana diatur dalam peraturan perundangan, data keuangan, data perjanjian kerahasiaan (*Non-Disclosure Agreement* atau NDA), prosedur operasional, rencana keberlangsungan kegiatan (*business continuity plan*), dokumen penawaran dan kontrak, hasil audit, hasil pengujian keamanan sistem;
   2) Perangkat lunak, meliputi: perangkat lunak aplikasi, perangkat lunak sistem, dan perangkat bantu pengembangan sistem;
   3) Aset fisik, meliputi: perangkat komputer, perangkat jaringan dan komunikasi, removable media, dan perangkat pendukung; dan
   4) Aset tak berwujud (*intangible*), meliputi: pengetahuan, pengalaman, keahlian, citra dan reputasi.

3. KEBIJAKAN
   a. Setiap pimpinan unit bertanggung jawab dalam mengatur dan menerapkan Tata Kelola Keamanan Informasi di lingkungan BKN di masing-masing lingkungan unit kerja setingkat pimpinan tinggi.
   b. Pimpinan unit TIK bertanggung jawab mengatur pelaksanaan pengamanan dan perlindungan aset informasi di lingkungan BKN.

4. STANDAR
   a. Catatan penerapan Tata Kelola Keamanan Informasi di lingkungan BKN:
      1) Unit TIK harus menggunakan catatan penerapan Tata Kelola Keamanan Informasi di lingkungan BKN untuk mengukur kepatuhan dan efektivitas penerapan Sistem Manajemen Keamanan Informasi.
      2) Catatan penerapan Tata Kelola Keamanan Informasi di lingkungan BKN harus meliputi:
         a) Formulir-formulir sesuai prosedur operasional yang dijalankan;
         b) Catatan gangguan keamanan informasi;
         c) Catatan dari sistem;

d) Catatan pengunjung di wilayah *secure areas*;
e) Kontrak dan perjanjian layanan;
f) Perjanjian kerahasiaan (*Non-Disclosure Agreement/ Confidentiality Agreements*); dan
g) Laporan Audit.

b. Penyusunan Dokumen Pendukung

Penyusunan dokumen pendukung kebijakan keamanan informasi harus memuat:

a) Tujuan dan ruang lingkup dokumen pendukung kebijakan keamanan informasi;
b) Kerangka kerja setiap tujuan/sasaran pengendalian keamanan informasi;
c) Metodologi penilaian risiko (*risk assessment*);
d) Penjelasan singkat mengenai standar, prosedur dan kepatuhan termasuk persyaratan peraturan yang harus dipenuhi, pengelolaan kelangsungan kegiatan, konsekuensi apabila terjadi pelanggaran;
e) Tanggung jawab setiap bagian terkait; dan
f) Dokumen referensi yang digunakan dalam menyusun dokumen pendukung kebijakan keamanan informasi.

c. Pengendalian Dokumen

1) Unit TIK harus mengendalikan dokumen Sistem Manajemen Keamanan Informasi Badan Kepegawaian Negara untuk menjaga kemutakhiran dokumen, efektivitas pelaksanaan operasional, menghindarkan dari segala jenis kerusakan, gangguan dan mencegah akses oleh pihak yang tidak berwenang.
2) Unit TIK menempatkan dokumen Sistem Manajemen Keamanan Informasi BKN di semua area operasional sehingga mudah diakses oleh pengguna di unit kerja masing-masing sesuai peruntukannya, kecuali yang memiliki klasifikasi sangat rahasia, rahasia atau terbatas harus ditempatkan pada area yang tidak mudah diakses.

E. PENGENDALIAN PENGELOLAAN ASET INFORMASI

1. TUJUAN

Pengelolaan aset informasi bertujuan memberikan pedoman dalam mengelola Aset Informasi di lingkungan BKN untuk melindungi dan menjamin keamanan aset informasi.

2. RUANG LINGKUP

Kebijakan dan standar pengelolaan aset informasi ini meliputi:

a. Tanggung jawab setiap unit kerja terhadap aset informasi; dan
b. Pengklasifikasian aset informasi.

3. KEBIJAKAN

a. Tanggung Jawab terhadap Aset Informasi
   1) Unit TIK mengidentifikasi aset informasi dan mendokumentasikan dalam daftar inventaris aset informasi. Daftar inventaris aset informasi dipelihara dan dikelola perubahannya oleh penanggung jawab pengendalian dokumen.
   2) Pimpinan unit kerja menetapkan pemilik aset informasi di setiap lingkungan unit kerjanya.
   3) Pimpinan unit kerja menetapkan aset informasi yang terkait dengan perangkat pengolah informasi.
   4) Pemilik Aset Informasi menetapkan aturan penggunaan aset informasi.

b. Klasifikasi Aset Informasi
   1) Aset informasi diklasifikasikan sesuai tingkat kerahasiaan, nilai, tingkat kekritisan, serta aspek hukumnya.
   2) Ketentuan rinci klasifikasi aset informasi diuraikan dalam standar pengelolaan aset informasi.
   3) Pemberian label klasifikasi aset informasi harus dilakukan secara konsisten terhadap seluruh aset informasi di lingkungan BKN.

4. STANDAR

Pengelolaan Aset Informasi

a. Pemilik Aset Informasi menetapkan dan mengkaji secara berkala klasifikasi aset informasi dan metode perlindungan keamanannya.

b. Pemilik Aset Informasi menetapkan pihak yang berwenang untuk mengakses aset informasi.

c. Dalam pengelolaan aset informasi BKN, aset informasi diklasifikasikan seperti pada tabel berikut:

Tabel Klasifikasi Aset Informasi

KLASIFIKASI ASET	KETERANGAN
SANGAT RAHASIA (*STRICTLY CONFIDENTIAL)*	Aset informasi BKN yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan menyebabkan kerugian pada strategi ketahanan nasional.
RAHASIA (*CONFIDENTIAL*)	Aset informasi BKN yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan mengganggu kelancaran kegiatan BKN atau mengganggu citra dan reputasi BKN dan/atau yang menurut peraturan perundang-undangan dinyatakan rahasia.
TERBATAS (*INTERNAL USE ONLY*)	Aset informasi BKN yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan mengganggu kelancaran kegiatan BKN namun tidak akan mengganggu citra dan reputasi BKN.
PUBLIK	Aset informasi BKN yang sengaja disediakan BKN untuk dapat diketahui masyarakat umum.

F. PENGENDALIAN ORGANISASI KEAMANAN INFORMASI

1. TUJUAN

Organisasi Keamanan Informasi bertujuan untuk memastikan tata kelola keamanan informasi di lingkungan BKN diimplementasikan secara efektif, efisien dan menyeluruh dengan menetapkan peran dan tanggung jawab keamanan informasi pada struktur yang ada (*ex officio*), serta dapat bekerja sama dengan pihak lain di luar lingkungan BKN.

2. RUANG LINGKUP

Kebijakan dan standar organisasi keamanan informasi ini meliputi:

a. Struktur organisasi keamanan informasi di lingkungan BKN;

b. Perjanjian kerahasiaan; dan

c. Hubungan dengan pihak berwenang, komunitas keamanan informasi, dan pihak ketiga.

3. KEBIJAKAN

a. Struktur Organisasi Keamanan Informasi

1) BKN menetapkan peran dan tanggung jawab keamanan informasi pada struktur yang ada sesuai dengan ketentuan peraturan perundang-undangan.

2) Kebijakan dan prosedur keamanan disusun oleh unit kerja yang memiliki tugas dan tanggung jawab keamanan informasi, ditetapkan oleh pimpinan, dan diimplementasikan di lingkungan BKN.

3) Pimpinan BKN berkomitmen dan mendukung implementasi dan operasional keamanan informasi melalui pengalokasian sumber daya yang memadai.

b. Perjanjian Kerahasiaan

1) Akses pada aset informasi yang berklasifikasi sangat rahasia, rahasia dan terbatas menggunakan perjanjian kerahasiaan (*Non-Disclosure Agreement*) di antara para pihak.

2) Pelanggaran perjanjian oleh salah satu pihak diselesaikan sesuai peraturan perundangan.

3) Berakhirnya perjanjian ditentukan berdasarkan masa retensi aset informasi yang diaksesnya.

c. Hubungan dengan pihak berwenang, komunitas keamanan informasi, dan pihak ketiga

1) Hubungan dengan pihak berwenang, komunitas keamanan informasi dan pihak ketiga dilandasi dengan prinsip kehati-hatian, menerapkan pengendalian keamanan informasi, dan sesuai dengan kepentingannya.

2) Kolaborasi dan kerja sama dengan pihak-pihak terkait dilaksanakan dalam rangka mendukung terselenggaranya keamanan informasi di lingkungan BKN.

4. STANDAR

a. Unit kerja yang memiliki tugas dan tanggung jawab keamanan informasi mengimplementasikan tata kelola berdasarkan pendekatan *Plan* (P) - *Do* (D) - *Check* (C) - *Action* (A).

b. Setiap unit kerja menerapkan program kerja atau kegiatan berdasarkan prinsip pengelolaan risiko *(risk management).*

c. Unit kerja yang memiliki tugas dan tanggung jawab keamanan informasi melakukan dokumentasi dari pengimplementasian tata kelola keamanan informasi.

d. Perjanjian Kerahasiaan

Perjanjian kerahasiaan harus memuat unsur-unsur sebagai berikut:

1) Definisi dari informasi yang akan dilindungi;
2) Durasi yang diharapkan dari sebuah perjanjian kerahasiaan;
3) Tanggung jawab dan tindakan penandatangan untuk menghindari pengungkapan informasi secara tidak sah;
4) Perlindungan kepemilikan informasi, rahasia organisasi, dan kekayaan intelektual;
5) Izin menggunakan informasi rahasia, dan hak-hak penandatangan untuk menggunakan informasi;
6) Hak untuk melakukan audit dan memantau kegiatan yang melibatkan informasi rahasia;
7) Proses untuk pemberitahuan dan pelaporan dari penyingkapan yang dilakukan secara tidak sah atau pelanggaran terhadap kerahasiaan informasi;
8) Tindakan yang diperlukan pada saat sebuah perjanjian kerahasiaan diakhiri;
9) Syarat-syarat untuk informasi yang akan dikembalikan atau dimusnahkan pada saat penghentian perjanjian; dan
10) Tindakan yang akan diambil apabila terjadi pelanggaran terhadap perjanjian kerahasiaan.

G. PENGENDALIAN KEAMANAN SUMBER DAYA MANUSIA

1. TUJUAN

Keamanan sumber daya manusia bertujuan memastikan bahwa seluruh pegawai dan pihak ketiga di lingkungan BKN memahami tanggung jawabnya masing-masing, sadar atas ancaman keamanan informasi, serta mengetahui proses terkait keamanan informasi sebelum, selama, dan setelah bertugas.

2. RUANG LINGKUP

Peran dan tanggung jawab seluruh pegawai dan pihak ketiga di lingkungan BKN yang harus dipahami dan dilaksanakan dalam implementasi keamanan informasi sesuai dengan ketentuan peraturan perundang-undangan.

3. KEBIJAKAN

a. Seluruh pegawai bertanggung jawab untuk menjaga keamanan informasi BKN sesuai dengan tugas dan fungsinya.

b. Pihak ketiga harus menyetujui dan menandatangani syarat dan perjanjian untuk menjaga keamanan informasi BKN.

c. Peran dan tanggung jawab pegawai dan pihak ketiga terhadap keamanan informasi didefinisikan, didokumentasikan, dan dikomunikasikan kepada yang bersangkutan.

d. Unit kerja akan melakukan pemeriksaan data pribadi yang diberikan oleh pegawai baru dan pihak ketiga sesuai dengan ketentuan peraturan perundang-undangan.

e. Seluruh pegawai harus mendapatkan peningkatan pengetahuan, dan sosialisasi keamanan informasi secara berkala sesuai tingkat tanggung jawabnya.

f. Pihak ketiga, jika diperlukan, mendapatkan sosialisasi untuk meningkatkan kepedulian terhadap keamanan informasi.

g. Seluruh pegawai dan pihak ketiga yang melanggar Tata Kelola Keamanan Informasi di lingkungan BKN akan dikenai sanksi atau tindakan disiplin sesuai ketentuan yang berlaku.

h. Seluruh pegawai yang berhenti bekerja atau mutasi dari unit kerja di lingkungan BKN harus mengembalikan seluruh aset informasi yang dipergunakan selama bekerja sesuai dengan ketentuan yang berlaku.

i. Pihak ketiga yang habis masa kontrak kerjanya harus mengembalikan seluruh aset informasi yang dipergunakan selama bekerja di lingkungan BKN.

j. Unit kerja harus menghentikan hak penggunaan aset informasi bagi pegawai yang sedang menjalani pemeriksaan yang terkait dengan dugaan pelanggaran Tata Kelola Keamanan Informasi di lingkungan BKN dan/atau yang sedang menjalani proses hukum.

k. Unit kerja harus mencabut hak akses terhadap aset informasi yang dimiliki pegawai dan pihak ketiga apabila yang bersangkutan tidak lagi bekerja di lingkungan BKN dan melaporkan pencabutan hak akses tersebut kepada unit kerja yang membidangi keamanan informasi.

4. STANDAR

Keamanan Sumber Daya Manusia meliputi:

a. Peran dan tanggung jawab pegawai terhadap keamanan informasi harus menjadi bagian dari penjabaran tugas dan fungsi, khususnya bagi yang memiliki akses terhadap aset informasi.

b. Pimpinan dari pegawai berkeahlian khusus atau yang berada di posisi kunci (*key person*) harus memastikan ketersediaan pengganti pegawai tersebut dengan kompetensi yang setara apabila pegawai yang bersangkutan mutasi/berhenti.

c. Peran dan tanggung jawab pegawai terhadap keamanan informasi harus menyertakan persyaratan untuk:
   1) Melaksanakan dan bertindak sesuai dengan organisasi keamanan informasi;
   2) Melindungi aset dari akses yang tidak sah, penyingkapan, modifikasi, kerusakan atau gangguan;
   3) Melaksanakan proses keamanan atau kegiatan keamanan informasi sesuai dengan peran dan tanggung jawabnya; dan
   4) Melaporkan kejadian, potensi kejadian, atau risiko keamanan informasi sesuai dengan Tata Kelola Keamanan Informasi di lingkungan BKN.

d. Pemeriksaan latar belakang calon pegawai dan pihak ketiga BKN harus memperhitungkan privasi, perlindungan data pribadi dan/atau pekerjaan berdasarkan undang-undang, meliputi:
   1) Ketersediaan referensi, dari referensi hubungan kerja dan referensi pribadi;
   2) Pemeriksaan kelengkapan dan ketepatan dari riwayat hidup pemohon;
   3) Konfirmasi kualifikasi akademik dan profesional yang diklaim;
   4) Pemeriksaan identitas; dan
   5) Pemeriksaan lebih rinci, seperti pemeriksaan dari catatan kriminal.

H. PENGENDALIAN KEAMANAN FISIK DAN LINGKUNGAN

1. TUJUAN

Keamanan fisik dan lingkungan bertujuan untuk mencegah akses fisik oleh pihak yang tidak berwenang, menghindari terjadinya kerusakan pada perangkat penyimpan, pengolah dan pengirim informasi serta gangguan pada aktivitas organisasi.

2. RUANG LINGKUP

Tata kelola keamanan fisik dan lingkungan ini meliputi:

a. Pengamanan area; dan
b. Pengamanan perangkat.

3. KEBIJAKAN

a. Pengamanan Area
   1) Seluruh pegawai, pihak ketiga, dan tamu yang memasuki lingkungan BKN harus mematuhi aturan yang berlaku di BKN.
   2) Ketentuan rinci tentang pengamanan area lingkungan kerja di BKN diuraikan dalam standar keamanan fisik dan lingkungan.

b. Pengamanan Perangkat
   1) Penempatan dan perlindungan perangkat
   2) Perangkat pengolah informasi dan perangkat pendukung harus ditempatkan di lokasi yang aman dan diposisikan sedemikian rupa untuk mengurangi risiko aset informasi dapat diakses oleh pihak yang tidak berwenang.
   3) Penempatan perangkat pengolah informasi dan perangkat pendukung yang berlokasi di luar lingkungan BKN harus mempertimbangkan aspek keamanan sesuai standar yang berlaku.
   4) Penyediaan perangkat pendukung
   5) Perangkat pendukung harus dipasang untuk menjamin beroperasinya perangkat pengolah informasi dan secara berkala harus diperiksa dan diuji ulang kinerjanya.
   6) Pengamanan kabel
      a) Kabel sumber daya listrik harus dilindungi dari kerusakan; dan
      b) Kabel telekomunikasi yang mengalirkan informasi harus dilindungi dari kerusakan dan penyadapan.
   7) Pemeliharaan perangkat
   8) Perangkat harus dipelihara secara berkala untuk menjamin ketersediaan, keutuhan, dan fungsinya.
   9) Pengamanan perangkat di luar lingkungan BKN.
   10) Penggunaan perangkat yang dibawa ke luar dari lingkungan BKN harus disetujui oleh Pejabat yang berwenang.

11) Pengamanan penggunaan kembali atau penghapusan/ pemusnahan perangkat
    a) Perangkat pengolah informasi penyimpan data yang sudah tidak digunakan lagi harus disanitasi sebelum digunakan kembali atau dihapuskan/dimusnahkan; dan
    b) Penanganan perangkat pengolah informasi penyimpan data di BKN sesuai dengan standar penanganan media penyimpan data.

4. STANDAR
    a. Perangkat harus dipelihara sesuai dengan petunjuk manualnya. Untuk pemeliharaan yang dilakukan oleh pihak ketiga, harus diadakan Perjanjian Tingkat Layanan (*Service Level Agreement*/SLA) yang mendefinisikan tingkat pemeliharaan yang disediakan dan tingkat kinerja yang harus dipenuhi pihak ketiga.
    b. Pemeliharaan terhadap perangkat keras atau perangkat lunak dilakukan hanya oleh pegawai yang berwenang.
    c. Dalam hal pemeliharaan perangkat tidak dapat dilakukan di tempat, maka pemindahan perangkat harus mendapatkan persetujuan Pejabat yang berwenang. Terhadap data yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA yang disimpan dalam perangkat tersebut harus dipindahkan terlebih dahulu.
    d. Otorisasi penggunaan perangkat harus dilakukan secara tertulis dan data-data yang terkait dengan aset informasi yang digunakan, seperti nama pemakai aset, lokasi, dan tujuan penggunaan aset, harus dicatat dan disimpan.
    e. Pengamanan Area
        1) Unit pengelola infrastruktur menyimpan perangkat pengolah informasi (*server*) di ruangan khusus (ruang *server*) yang dilindungi dengan pengamanan fisik yang memadai antara lain pintu elektronik, sistem pemadam kebakaran, alarm bahaya dan perangkat pemutus aliran listrik;
        2) Akses ke ruang *server*/*data center*, dan area kerja yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus dibatasi dan hanya diberikan kepada pegawai yang berwenang;

3) Pihak ketiga yang memasuki *server/data center*, dan area kerja yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus didampingi pegawai unit pengelola infrastruktur sepanjang waktu kunjungan. Waktu masuk dan keluar serta maksud kedatangan harus dicatat dalam buku catatan kunjungan;
4) Kantor, ruangan, dan perangkat yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus dilindungi secara memadai;
5) Pegawai dan pihak ketiga tidak diizinkan merokok, makan, minum di ruang *server*/area *data center*; dan
6) Area keluar masuk barang dan area publik harus selalu dijaga, diawasi dan dikendalikan, dan jika memungkinkan disterilkan dari perangkat pengolah informasi untuk menghindari akses oleh pihak yang tidak berwenang.

f. Pengamanan Kantor, Ruangan, dan Fasilitas Pengamanan Kantor, Ruangan, dan Fasilitas mencakup:
1) Pengamanan kantor, ruangan, dan fasilitas harus sesuai dengan peraturan dan standar keamanan dan keselamatan kerja yang berlaku;
2) Fasilitas utama harus ditempatkan khusus untuk menghindari akses publik;
3) Pembatasan pemberian identitas atau tanda-tanda keberadaan aktivitas pengolahan informasi; dan
4) Direktori dan buku telepon internal untuk mengidentifikasi lokasi perangkat pengolah informasi tidak mudah diakses oleh publik.

g. Perlindungan terhadap Ancaman Eksternal dan Lingkungan
Perlindungan terhadap ancaman eksternal dan lingkungan harus mempertimbangkan:
1) Bahan-bahan berbahaya atau mudah terbakar harus disimpan pada jarak yang aman dari secure areas;
2) Perlengkapan umum seperti alat tulis tidak boleh disimpan dalam secure areas;
3) Perangkat media backup harus diletakkan pada jarak yang aman untuk menghindari kerusakan dari bencana yang mempengaruhi fasilitas utama; dan
4) Perangkat pemadam kebakaran harus disediakan dan diletakkan di tempat yang tepat.

h. Penempatan dan Perlindungan Perangkat

Penempatan dan perlindungan perangkat harus mencakup:

1) Perangkat harus diletakkan pada lokasi yang meminimalkan akses yang tidak perlu ke dalam area kerja;
2) Perangkat pengolah informasi yang menangani informasi sensitif harus diposisikan dan dibatasi arah sudut pandangnya untuk mengurangi risiko informasi dilihat oleh pihak yang tidak berwenang selama digunakan, dan perangkat penyimpanan diamankan untuk menghindari akses oleh pihak yang tidak berwenang;
3) Perangkat yang memerlukan perlindungan khusus seperti perangkat jaringan di luar ruang *server*/area *data center* harus terisolasi untuk mengurangi tingkat perlindungan/ perlakuan standar yang perlu dilakukan;
4) Langkah-langkah pengendalian dilakukan untuk meminimalkan risiko potensi ancaman fisik, seperti pencurian, api, bahan peledak, asap, air termasuk kegagalan penyediaan air, debu, getaran, efek kimia, gangguan pasokan listrik, gangguan komunikasi, radiasi elektromagnetik, dan perusakan;
5) Kondisi lingkungan, seperti suhu dan kelembaban harus dimonitor untuk mencegah perubahan kondisi yang dapat mempengaruhi pengoperasian perangkat pengolah informasi;
6) Perlindungan petir harus diterapkan untuk semua bangunan dan filter perlindungan petir harus dipasang untuk semua jalur komunikasi dan listrik; dan
7) Perangkat pengolah informasi sensitif harus dilindungi untuk meminimalkan risiko kebocoran informasi.

i. Pengamanan Kabel

Perlindungan keamanan kabel mencakup:

1) Pemasangan kabel sumber daya listrik dan kabel telekomunikasi ke perangkat pengolah informasi selama memungkinkan harus terletak di bawah tanah, atau menerapkan alternatif perlindungan lain yang memadai;
2) Pemasangan kabel jaringan harus dilindungi dari penyusupan yang tidak sah atau kerusakan, misalnya dengan menggunakan conduit atau menghindari rute melalui area publik;

3) Pemisahan antara kabel sumber daya listrik dengan kabel telekomunikasi untuk mencegah interferensi;
4) Penandaan/penanaman kabel dan perangkat harus diterapkan secara jelas untuk memudahkan penanganan kesalahan;
5) Penggunaan dokumentasi daftar panel patch diperlukan untuk mengurangi kesalahan; dan
6) Pengendalian untuk sistem informasi yang sensitif harus mempertimbangkan:
   a) Penggunaan *conduit*;
   b) Penggunaan ruangan terkunci pada tempat inspeksi dan titik pemutusan kabel;
   c) Penggunaan rute alternatif dan/atau media transmisi yang menyediakan keamanan yang sesuai;
   d) Penggunaan conduit;
   e) Penggunaan ruangan terkunci pada tempat inspeksi dan titik pemutusan kabel;
   f) Penggunaan rute alternatif dan/atau media transmisi yang menyediakan keamanan yang sesuai;

I. PENGENDALIAN PENGELOLAAN KOMUNIKASI DAN OPERASIONAL

1. TUJUAN

Pengelolaan komunikasi dan operasional bertujuan untuk memastikan operasional yang aman dan benar pada perangkat pengolah informasi, mengimplementasikan dan memelihara keamanan informasi, mengelola layanan yang diberikan pihak ketiga, meminimalkan risiko kegagalan, melindungi keutuhan dan ketersediaan informasi, memastikan keamanan pertukaran informasi, dan pemantauan terhadap proses operasional.

2. RUANG LINGKUP

a. Prosedur operasional dan tanggung jawab;
b. Pengelolaan layanan oleh pihak ketiga;
c. Perencanaan dan penerimaan sistem;
d. Perlindungan terhadap ancaman program yang membahayakan;
e. Pencadangan (*backup*);
f. Pengelolaan keamanan jaringan;
g. Penanganan media penyimpan data;
h. Pertukaran informasi; dan
i. Pemantauan.

3. KEBIJAKAN

a. Prosedur Operasional dan Tanggung Jawab

1) Dokumentasi Prosedur Operasional

Unit TIK dan unit kerja harus mendokumentasikan, memelihara, menyediakan seluruh prosedur operasional terkait dengan penggunaan perangkat penyimpan, dan pengolah informasi bagi pengguna sesuai dengan peruntukannya.

2) Pengelolaan Perubahan Layanan TIK

Unit TIK dan unit kerja harus mengendalikan perubahan terhadap perangkat pengolah informasi.

Pengelolaan perubahan layanan TIK di BKN akan ditetapkan dalam ketentuan tersendiri.

3) Pemisahan Tugas

Unit kerja harus melakukan pemisahan tugas untuk proses yang melibatkan informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA untuk menghindari adanya pegawai yang memiliki pengendalian eksklusif terhadap seluruh aset informasi dan perangkat pengolahnya.

4) Pemisahan Perangkat Pengembangan dan Operasional

Unit TIK harus melakukan pemisahan perangkat pengembangan, pengujian, dan operasional untuk mengurangi risiko perubahan atau akses oleh pihak yang tidak berwenang terhadap sistem operasional.

b. Pengelolaan Layanan oleh Pihak Ketiga

1) Penyediaan layanan

Unit kerja harus memastikan bahwa pengendalian keamanan informasi, definisi layanan, dan tingkat layanan yang tercantum dalam kesepakatan penyediaan layanan telah diterapkan, dioperasikan, dan dipelihara oleh pihak ketiga.

2) Pemantauan dan kajian layanan pihak ketiga

Unit kerja harus melakukan pemantauan dan kajian terhadap kinerja penyediaan layanan, laporan, dan catatan yang disediakan oleh pihak ketiga secara berkala.

3) Pengelolaan perubahan pada layanan pihak ketiga
Unit kerja harus memperhatikan kritikalitas, proses yang terkait, dan hasil penilaian ulang risiko layanan apabila terjadi perubahan pada layanan yang disediakan pihak ketiga.

c. Perencanaan dan Penerimaan Sistem
Kegiatan perencanaan dan penerimaan sistem meliputi:
1) Pengelolaan kapasitas dalam rangka perencanaan sistem
a) Unit TIK harus memantau penggunaan perangkat pengolah informasi dan membuat perkiraan pertumbuhan kebutuhan ke depan untuk memastikan ketersediaan kapasitas; dan
b) Pengelolaan kapasitas di BKN akan ditetapkan dalam ketentuan tersendiri.
2) Penerimaan sistem
a) Unit TIK harus menetapkan kriteria penerimaan (*acceptance criteria*) untuk sistem informasi baru, pemutakhiran (*upgrade*) dan versi baru serta melakukan pengujian sebelum penerimaan; dan
b) Penerimaan sistem di BKN akan ditetapkan dalam ketentuan tersendiri.

d. Perlindungan terhadap ancaman program yang membahayakan
1) Unit TIK harus menerapkan sistem yang dapat melakukan pendeteksian, pencegahan, dan pemulihan sebagai bentuk perlindungan terhadap ancaman program yang membahayakan *(malicious code)*.
2) Perlindungan terhadap ancaman program yang membahayakan (*malicious code*) di Badan Kepegawaian Negara ditetapkan dalam ketentuan tersendiri.

e. Pencadangan (*Backup)*
1) Unit TIK harus melakukan backup informasi dan perangkat lunak yang berada di Pusat Data/*Data Center* secara berkala.
2) Proses *backup* di BKN sesuai dengan standar *backup* yang ditetapkan dalam prosedur operasional standar operasional *data center* BKN.

f. Pengelolaan Keamanan Jaringan

1) Pengendalian Jaringan

a) Unit TIK dan unit kerja harus mengelola dan melindungi jaringan dari berbagai bentuk ancaman; dan

b) Ketentuan rinci pengendalian jaringan di BKN diuraikan dalam standar pengelolaan komunikasi dan operasional.

2) Keamanan Layanan Jaringan

Unit TIK harus mengidentifikasi fitur keamanan layanan, tingkat layanan, dan kebutuhan pengelolaan serta mencantumkannya dalam kesepakatan penyediaan layanan jaringan termasuk layanan jaringan yang disediakan oleh pihak ketiga.

g. Penanganan Media Penyimpan Data

1) Unit kerja setingkat mematuhi prosedur penanganan media penyimpan data untuk melindungi aset informasi.

2) Penanganan media penyimpanan data di Badan Kepegawaian Negara sesuai dengan ketetapan standar penanganan media penyimpanan data.

h. Pertukaran Informasi

1) Pertukaran informasi dan perangkat lunak antara BKN dengan pihak ketiga hanya akan dilakukan atas kesepakatan tertulis kedua belah pihak.

2) Unit kerja harus melakukan penilaian risiko yang memadai sebelum melaksanakan pertukaran informasi.

3) Unit kerja harus menerapkan pengendalian keamanan informasi untuk pengiriman informasi melalui surat elektronik atau pengiriman informasi melalui jasa layanan pengiriman dalam rangka menghindari akses pihak yang tidak berwenang.

4) Ketentuan rinci pertukaran informasi di BKN diuraikan dalam standar pengelolaan komunikasi dan operasional.

i. Pemantauan

1) Audit *Logging*

Unit TIK harus menerapkan audit logging yang mencatat aktivitas pengguna, pengecualian, dan kejadian keamanan informasi dalam kurun waktu tertentu untuk membantu pengendalian akses dan investigasi di masa mendatang.

2) Memantau Penggunaan Sistem

Unit TIK harus memantau penggunaan sistem dan mengkaji secara berkala hasil kegiatan pemantauan.

3) Perlindungan Data Catatan

Unit TIK harus melindungi fasilitas pencatatan dan data yang dicatat dari kerusakan dan akses oleh pihak yang tidak berwenang.

4) Pencatatan Kegiatan *System Administrator* dan *System Operator*

Unit TIK harus menerapkan pencatatan kegiatan system administrator dan *system operator*.

5) Pencatatan Kesalahan

Unit TIK harus menerapkan pencatatan kesalahan untuk dianalisis dan diambil tindakan penanganan yang tepat.

6) Sinkronisasi Waktu

Unit TIK harus memastikan semua perangkat pengolah informasi yang tersambung dengan jaringan telah disinkronisasi dengan sumber waktu yang akurat dan disepakati.

4. STANDAR

a. Dokumentasi Prosedur Operasional

Prosedur operasional meliputi:

1) Tata cara pengolahan dan penanganan informasi;
2) Tata cara menangani kesalahan-kesalahan atau kondisi khusus yang terjadi beserta pihak yang harus dihubungi bila mengalami kesulitan teknis;
3) Cara memfungsikan kembali perangkat dan cara mengembalikan perangkat ke keadaan awal saat terjadi kegagalan sistem;
4) Tata cara *backup* dan *restore*; dan
5) Tata cara pengelolaan jejak audit (*audit trails*) pengguna dan catatan kejadian/kegiatan sistem.

b. Pemisahan Perangkat Pengembangan dan Operasional

Pemisahan perangkat pengembangan dan operasional harus mempertimbangkan:

1) Pengembangan dan operasional perangkat lunak harus dioperasikan di sistem atau prosesor komputer dan domain atau direktori yang berbeda;
2) Instruksi Kerja (*working instruction*) rilis dari pengembangan perangkat lunak ke operasional harus ditetapkan dan didokumentasikan;
3) *Compiler*, editor, dan alat bantu pengembangan lain tidak boleh diakses dari sistem operasional ketika tidak dibutuhkan;
4) Lingkungan sistem pengujian harus diusahakan sama dengan lingkungan sistem operasional;
5) Pengguna harus menggunakan profil pengguna yang berbeda untuk sistem pengujian dan sistem operasional, serta aplikasi harus menampilkan pesan identifikasi dari sistem untuk mengurangi risiko kesalahan; dan
6) Data yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA tidak boleh disalin ke dalam lingkungan pengujian sistem.

c. Pemantauan dan Pengkajian Layanan Pihak Ketiga

Pemantauan dan pengkajian layanan dari pihak ketiga, serta laporan dan catatan dari pihak ketiga mencakup proses sebagai berikut:

1) Pemantauan tingkat kinerja layanan untuk memastikan kesesuaian kepatuhan dengan perjanjian;
2) Pengkajian laporan layanan pihak ketiga dan pengaturan pertemuan berkala dalam rangka pembahasan perkembangan layanan sebagaimana diatur dalam perjanjian/kesepakatan;
3) Pemberian informasi tentang gangguan keamanan informasi dan pengkajian informasi ini bersama pihak ketiga sebagaimana diatur dalam perjanjian/kesepakatan;
4) Pemeriksaan jejak audit pihak ketiga dan pencatatan peristiwa keamanan, masalah operasional, kegagalan, dan gangguan yang terkait dengan layanan yang diberikan; dan
5) Penyelesaian dan pengelolaan masalah yang teridentifikasi.

d. Pengelolaan Keamanan Jaringan

Pengelolaan keamanan jaringan mencakup:

1) Pemantauan kegiatan pengelolaan jaringan untuk menjamin bahwa perangkat jaringan digunakan secara efektif dan efisien;
2) Pengendalian dan pengaturan tentang penyambungan atau perluasan jaringan internal atau eksternal BKN;
3) Pengendalian dan pengaturan akses ke sistem jaringan internal atau eksternal BKN;
4) Pencatatan informasi pihak ketiga yang diizinkan mengakses ke jaringan BKN dan menerapkan pemantauan serta pencatatan kegiatan selama menggunakan jaringan;
5) Pemutusan layanan tanpa pemberitahuan jika terjadi gangguan keamanan informasi;
6) Perlindungan jaringan dari akses yang tidak berwenang mencakup:
   a) Penetapan untuk penanggung jawab pengelolaan jaringan dipisahkan dari pengelolaan perangkat pengolah informasi;
   b) Penerapan pengendalian khusus untuk melindungi keutuhan informasi yang melewati jaringan umum antara lain dengan penggunaan enkripsi; dan
   c) Pendokumentasian arsitektur jaringan seluruh komponen perangkat keras jaringan dan perangkat lunak.
7) Penerapan fitur keamanan layanan jaringan mencakup:
   a) Teknologi keamanan seperti autentikasi, enkripsi, dan pengendalian sambungan jaringan;
   b) Parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan sesuai dengan keamanan dan aturan koneksi jaringan; dan
   c) Prosedur untuk penggunaan layanan jaringan yang membatasi akses ke layanan jaringan atau aplikasi.

e. Pertukaran Informasi

1) Prosedur pertukaran informasi bila menggunakan perangkat komunikasi elektronik, mencakup:
   a) Perlindungan pertukaran informasi dari pencegahan, penyalinan, modifikasi, *miss-routing*, dan perusakan;

b) Pendeteksian dan perlindungan terhadap kode berbahaya yang dapat dikirim melalui penggunaan komunikasi elektronik;

c) Perlindungan informasi elektronik dalam bentuk *attachment* yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA;

d) Pertimbangan risiko terkait penggunaan perangkat komunikasi nirkabel;

2) Pertukaran informasi yang tidak menggunakan perangkat komunikasi elektronik, mengacu pada ketentuan yang berlaku.

3) Pengendalian pertukaran informasi bila menggunakan perangkat komunikasi elektronik, mencakup:

a) Pencegahan terhadap penyalahgunaan wewenang pegawai dan pihak ketiga yang dapat membahayakan organisasi;

b) Penggunaan teknik kriptografi;

c) Penyelenggaraan penyimpanan dan penghapusan/ pemusnahan untuk semua korespondensi kegiatan, termasuk pesan, yang sesuai dengan ketentuan yang berlaku;

d) Larangan meninggalkan informasi sensitif pada perangkat pengolah informasi;

e) Pembatasan penerusan informasi secara otomatis;

f) Pembangunan kepedulian atas ancaman pencurian informasi, misalnya terhadap:

(1) Pengungkapan informasi sensitif untuk menghindari mencuri dengar saat melakukan panggilan telepon;

(2) Akses pesan di luar kewenangannya;

(3) Pengiriman dokumen dan pesan ke tujuan yang salah.

4) Pembangunan kepedulian atas pendaftaran data demografis, seperti alamat surat elektronik atau informasi pribadi lainnya untuk menghindari pengumpulan informasi yang tidak sah; dan

5) Penyediaan informasi internal Badan Kepegawaian Negara bagi masyarakat umum harus disetujui oleh pemilik informasi dan sesuai dengan ketentuan yang berlaku.

f. Pemantauan

Prosedur pemantauan penggunaan sistem pengolah informasi ditetapkan untuk menjamin agar kegiatan akses yang tidak sah tidak perlu terjadi. Prosedur ini mencakup pemantauan:

1) Kegagalan akses *(access failures);*
2) Anomali login dengan pola penggunaan tidak wajar;
3) Alokasi dan penggunaan hak akses khusus;
4) Penelusuran transaksi dan pengiriman *file* tertentu yang mencurigakan; dan
5) Penggunaan sumber daya sensitif.

J. PENGENDALIAN AKSES

1. TUJUAN

Pengendalian akses bertujuan untuk memastikan otorisasi akses pengguna dan mencegah akses pihak yang tidak berwenang terhadap aset informasi khususnya perangkat pengolah informasi.

2. RUANG LINGKUP

Kebijakan dan standar pengendalian akses ini meliputi:

a. Persyaratan untuk pengendalian akses;
b. Pengelolaan akses pengguna;
c. Tanggung jawab pengguna;
d. Pengendalian akses jaringan;
e. Pengendalian akses ke sistem operasi;
f. Pengendalian akses ke aplikasi dan sistem informasi; dan
g. Mobile *computing* dan *Teleworking*.

3. KEBIJAKAN

a. Persyaratan untuk Pengendalian Akses

Unit kerja pemilik risiko harus menyusun, mendokumentasikan, dan mengkaji ketentuan akses ke aset informasi berdasarkan kebutuhan organisasi dan persyaratan keamanan.

b. Pengelolaan Akses Pengguna

1) Pendaftaran Pengguna

Unit kerja yang membidangi keamanan informasi menyusun prosedur pengelolaan hak akses pengguna sesuai dengan peruntukannya.

2) Pengelolaan Hak Akses Khusus

Unit kerja yang membidangi keamanan informasi harus membatasi dan mengendalikan penggunaan hak akses khusus.

3) Pengelolaan Kata Sandi Pengguna

a) Unit kerja yang membidangi keamanan informasi harus mengatur pengelolaan kata sandi pengguna; dan

b) Pengelolaan kata sandi pengguna sesuai standar yang ditetapkan unit kerja yang membidangi keamanan informasi.

4) Kajian Hak Akses Pengguna

Unit kerja yang membidangi keamanan informasi bersama unit pemilik risiko harus memantau dan mengevaluasi hak akses pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya.

c. Tanggung Jawab Pengguna

1) Pengguna harus mematuhi aturan pembuatan dan penggunaan kata sandi. Tanggung jawab pengguna terhadap kata sandi sesuai dengan standar tanggung jawab pengguna yang ditetapkan unit kerja yang membidangi keamanan informasi;

2) Pengguna harus memastikan perangkat pengolah informasi yang digunakan mendapat perlindungan terutama pada saat ditinggalkan; dan

3) Pengguna harus melindungi informasi agar tidak diakses oleh pihak yang tidak berwenang.

d. Pengendalian Akses Jaringan

1) Penggunaan Layanan Jaringan

Unit kerja yang membidangi keamanan informasi harus mengatur akses pengguna dalam memanfaatkan layanan jaringan komunikasi dan internet BKN sesuai peruntukannya.

2) Otorisasi Pengguna Untuk Koneksi Eksternal

Unit kerja yang membidangi keamanan informasi harus menerapkan proses otorisasi pengguna untuk setiap akses ke dalam jaringan internal melalui koneksi eksternal (*remote access* dan atau *Virtual Private Network).*

3) Pemisahan Dalam Jaringan

Unit kerja yang membidangi keamanan informasi harus memisahkan jaringan untuk pengguna, dan sistem informasi.

4) Pengendalian Koneksi Jaringan

Unit kerja yang membidangi keamanan informasi harus menerapkan mekanisme pengendalian akses pengguna sesuai dengan persyaratan pengendalian akses.

5) Pengendalian *Routing* Jaringan

Pengendalian *routing* jaringan internal BKN harus dilakukan sesuai pengendalian akses dan kebutuhan layanan informasi.

e. Pengendalian Akses ke Sistem Operasi

1) Prosedur Akses yang Aman

Akses ke sistem operasi harus dikontrol dengan menggunakan prosedur akses yang aman.

2) Identifikasi dan Otorisasi Pengguna

a) Setiap pengguna harus memiliki akun yang unik dan hanya digunakan sesuai dengan peruntukannya; dan

b) Proses otorisasi pengguna harus menggunakan teknik autentikasi yang sesuai untuk memvalidasi identitas dari pengguna.

3) Sistem Pengelolaan Kata Sandi

Sistem pengelolaan kata sandi harus mudah digunakan dan dapat memastikan kualitas kata sandi yang dibuat pengguna.

4) Penggunaan *System Utilities*

Unit kerja yang membidangi keamanan informasi harus mengendalikan penggunaan *system utilities.*

5) Session *Time-Out*

Fasilitas *session time-out* harus diaktifkan untuk menutup dan mengunci layar komputer, aplikasi, dan koneksi jaringan apabila tidak ada aktivitas pengguna setelah periode tertentu.

6) Pembatasan Waktu Koneksi

Unit kerja yang membidangi keamanan informasi harus membatasi waktu koneksi untuk sistem informasi atau aplikasi yang memiliki klasifikasi SANGAT RAHASIA.

f. Pengendalian akses ke aplikasi dan sistem informasi
g. *Mobile Computing* dan *Teleworking*.

4. STANDAR

a. Persyaratan untuk Pengendalian Akses

Persyaratan pengendalian akses mencakup penentuan kebutuhan keamanan dari pengolah aset informasi.

b. Pengelolaan Akses Pengguna

Prosedur pengelolaan akses pengguna harus mencakup:

1) Penggunaan akun yang unik untuk mengaktifkan pengguna agar terhubung dengan sistem informasi atau layanan, dan pengguna dapat bertanggung jawab dalam penggunaan sistem informasi atau layanan tersebut. Penggunaan akun khusus hanya diperbolehkan sebatas yang diperlukan untuk kegiatan atau alasan operasional, dan harus disetujui pejabat yang berwenang serta didokumentasikan;
2) Pemeriksaan bahwa pengguna memiliki otorisasi dari pemilik sistem untuk menggunakan sistem informasi atau layanan, dan jika diperlukan harus mendapat persetujuan yang terpisah dari pejabat yang berwenang;
3) Penghapusan atau penonaktifan akses pengguna yang telah berubah tugas dan/atau fungsinya, setelah penugasan berakhir atau mutasi;
4) Pemeriksaan, penghapusan, serta penonaktifan akun secara berkala dan untuk pengguna yang memiliki lebih dari 1 (satu) akun; dan
5) Pemastian bahwa akun tidak digunakan oleh pengguna lain.

c. Pengelolaan Hak Akses Khusus (*privilege management*)

1) Hak akses khusus setiap sistem dari pabrikan perlu diidentifikasi untuk diberikan kepada pengguna yang terkait dengan produk, seperti sistem operasi, sistem pengelolaan basis data dan aplikasi;
2) Hak akses khusus hanya diberikan kepada pengguna sesuai dengan peruntukannya berdasarkan kebutuhan dan kegiatan tertentu;

3) Hak akses khusus diberikan secara terpisah dari akun yang digunakan untuk kegiatan umum, seperti akun *system administrator, database administrator, dan network administrator*.

d. Kajian Hak Akses Pengguna

Hak akses pengguna harus mempertimbangkan:

1) Hak akses pengguna harus dikaji paling sedikit 6 (enam) bulan sekali atau setelah terjadi perubahan pada sistem, status kepegawaian pengguna, atau struktur organisasi;
2) Hak akses khusus harus dikaji paling sedikit 6 (enam) bulan sekali dalam jangka waktu lebih sering dibanding jangka waktu pengkajian hak akses atau setelah terjadi perubahan pada sistem, status kepegawaian pengguna, atau struktur organisasi; dan
3) Pemeriksaan hak akses khusus harus dilakukan secara berkala, untuk memastikan pemberian hak akses khusus telah diotorisasi.

e. Pengendalian Akses Jaringan

1) Menerapkan prosedur otorisasi untuk pemberian akses ke jaringan dan layanan jaringan;
2) Menerapkan teknik autentikasi akses dari koneksi eksternal; dan
3) Melakukan penghentian/isolasi layanan jaringan pada area jaringan yang mengalami gangguan keamanan informasi.

f. Pemisahan Dalam Jaringan

Melakukan pemisahan dalam jaringan antara lain:

1) Pemisahan berdasarkan kelompok layanan informasi, pengguna, dan aplikasi; dan
2) Pemberian akses jaringan kepada tamu, hanya dapat diberikan akses terbatas misalnya internet dan/atau surat elektronik tanpa bisa terhubung ke jaringan internal BKN.

g. Mobile *Computing* dan *Teleworking*

1) Penggunaan perangkat *mobile computing* dan *teleworking* harus mempertimbangkan:
   a) Memenuhi keamanan informasi dalam penentuan lokasi;

b) Menjaga keamanan akses;
c) Menggunakan anti *malicious code*;
d) Memakai perangkat lunak berlisensi; dan
e) Mendapat persetujuan Pejabat yang berwenang/ atasan langsung pegawai.

2) Pencabutan hak akses dan pengembalian fasilitas perangkat *teleworking* apabila kegiatan telah selesai.

K. PENGENDALIAN KEAMANAN INFORMASI DALAM PENGADAAN, PENGEMBANGAN, DAN PEMELIHARAAN SISTEM INFORMASI

1. TUJUAN

Keamanan informasi dalam pengadaan, pengembangan, dan pemeliharaan sistem informasi bertujuan untuk memastikan bahwa keamanan informasi merupakan bagian yang terintegrasi dengan sistem informasi, mencegah terjadinya kesalahan, kehilangan, serta modifikasi oleh pihak yang tidak berwenang.

2. RUANG LINGKUP

a. Pengolahan informasi pada aplikasi;
b. Pengendalian penggunaan kriptografi;
c. Keamanan sistem file (*file system*);
d. Keamanan dalam proses pengembangan dan pendukung (*support process*); dan
e. Pengelolaan kerentanan teknis.

3. KEBIJAKAN

Pengadaan, pengembangan dan pemeliharaan sistem informasi harus memenuhi persyaratan sebagai berikut:

a. Keamanan Sistem Informasi

Unit infrastruktur dan keamanan TI dan unit kerja menetapkan dan mendokumentasikan secara jelas persyaratan keamanan informasi yang relevan sebelum pengadaan, pengembangan, atau pemeliharaan sistem informasi baru.

b. Pengolahan Informasi pada Aplikasi

Proses validasi perlu dilakukan untuk memastikan data yang diproses benar, utuh dan sesuai. Validasi informasi mencakup:

1) Validasi data yang masuk;
2) Pengendalian proses internal; dan
3) Validasi data keluaran.

c. Pengendalian Penggunaan Kriptografi

1) Unit kerja harus menerapkan sistem kriptografi dalam setiap pengembangan aplikasi untuk perlindungan informasi sesuai *best practises* yang direkomendasikan oleh unit yang membidangi keamanan informasi.
2) Sistem kriptografi digunakan untuk melindungi aset informasi yang memiliki klasifikasi SANGAT RAHASIA, RAHASIA, dan TERBATAS.

d. Keamanan File Sistem

1) Pengendalian operasional perangkat lunak;
2) Perlindungan terhadap sistem pengujian data; dan
3) Pengendalian akses ke kode program (*source code*).

Unit kerja dalam melaksanakan pengembangan sistem atau aplikasi yang dikembangkan harus mengendalikan akses ke kode program (*source code*) secara ketat dan disimpan di tempat yang aman.

e. Keamanan dalam Proses Pengembangan dan Pendukung

1) Prosedur pengendalian perubahan sistem operasi

   Unit kerja dalam melaksanakan pengembangan sistem/aplikasi harus mengendalikan perubahan pada sistem operasi dengan penggunaan prosedur pengendalian perubahan.
2) Prosedur pengendalian perubahan pada perangkat lunak
3) Kajian teknis aplikasi setelah perubahan sistem operasi dan/atau perangkat lunak

   Unit kerja harus meninjau dan menguji sistem operasi dan atau perangkat lunak untuk memastikan tidak ada dampak merugikan pada proses operasional atau keamanan informasi pada saat terjadi perubahan sistem operasi dan/atau perangkat lunak.
4) Kebocoran informasi

   Unit kerja harus mencegah kemungkinan terjadinya kebocoran informasi.
5) Pengembangan perangkat lunak oleh pihak ketiga

   Unit kerja yang membidangi pengembangan sistem informasi dan unit kerja pemilik sistem/aplikasi harus melakukan supervisi dan memantau pengembangan sistem/perangkat lunak yang dilakukan oleh pihak ketiga.

f. Pengelolaan Kerentanan Teknis

1) Unit kerja yang membidangi keamanan informasi harus melakukan penilaian kerentanan dan pengujian keamanan, penilaian risiko, dan menetapkan pengendalian risiko *(vulnerability assessment* dan *penetration testing)* pada sistem informasi maupun komponen pendukung yang digunakan di Badan Kepegawaian Negara.

2) Unit kerja pemilik aplikasi harus melakukan remediasi atau perbaikan sistem informasi/aplikasi berdasarkan hasil temuan kerentanan *(vulnerability assessment* dan *penetration testing).* Dalam melakukan perbaikan kerentanan teknis dapat berkonsultasi dan berkoordinasi dengan unit kerja yang membidangi pengembangan sistem informasi.

4. STANDAR

a. Spesifikasi kebutuhan perangkat pengolah informasi yang dikembangkan baik oleh internal atau pihak ketiga harus didokumentasikan secara formal.

b. Pemrosesan Data pada Aplikasi

Pemeriksaan data masukan harus mempertimbangkan:

1) Penerapan mekanisme pengecekan masukan untuk mendeteksi kesalahan berikut:
   a) Karakter tidak valid dalam *field* data;
   b) Di luar rentang/batas *value* yang diperbolehkan;
   c) Data tidak lengkap;
   d) Melewati batas volume data; dan
   e) Data yang tidak diotorisasi dan tidak konsisten.
2) Menampilkan pesan yang sesuai dalam menanggapi kesalahan validasi;
3) Sistem mampu membuat dan mengeluarkan catatan aktivitas terkait proses perekaman data.

c. Keamanan file sistem

Proses pemutakhiran perangkat lunak operasional, aplikasi, library program hanya boleh dilakukan oleh *system administrator* setelah melalui proses otorisasi;

L. PENGENDALIAN PENGELOLAAN GANGGUAN KEAMANAN INFORMASI

1. TUJUAN

Pengelolaan gangguan keamanan informasi bertujuan untuk memastikan kejadian dan kelemahan keamanan informasi yang terhubung dengan sistem informasi dikomunikasikan untuk dilakukan perbaikan, serta dilakukan pendekatan yang konsisten dan efektif agar dapat dihindari atau tidak terulang kembali.

2. RUANG LINGKUP

a. Pelaporan kejadian dan kelemahan keamanan informasi; dan
b. Pengelolaan gangguan keamanan informasi dan perbaikannya.

Secara detail diatur dalam ketentuan teknis BKN-CSIRT *(Computer Security Incident Response Team)*.

3. KEBIJAKAN

a. Pelaporan Kejadian dan Kelemahan Keamanan Informasi; dan
b. Pengelolaan Gangguan Keamanan Informasi dan Perbaikannya.

Secara detail diatur dalam ketentuan teknis BKN-CSIRT *(Computer Security Incident Response Team)*.

4. STANDAR

a. Pelaporan Kejadian dan Kelemahan Keamanan Informasi
    1) Gangguan keamanan informasi antara lain:
        a) Hilangnya layanan, perangkat, atau fasilitas TIK;
        b) Kerusakan fungsi sistem atau kelebihan beban;
        c) Perubahan sistem di luar kendali;
        d) Kerusakan fungsi perangkat lunak atau perangkat keras;
        e) Pelanggaran akses ke dalam sistem pengolah informasi TIK;
        f) Kelalaian manusia; dan
        g) Ketidaksesuaian dengan ketentuan yang berlaku.
    2) Pegawai dan pihak ketiga harus menyadari tanggung jawab mereka untuk melaporkan setiap gangguan keamanan informasi secepat mungkin.
        a) Pelaporan gangguan mencakup:
            (1) Proses umpan balik yang sesuai untuk memastikan bahwa pihak yang melaporkan kejadian keamanan informasi mendapatkan pemberitahuan penanganan masalah;

(2) Formulir laporan gangguan keamanan informasi untuk mendukung tindakan pelaporan dan membantu pelapor mengingat kronologis kejadian keamanan informasi;

(3) Perilaku yang benar dalam menghadapi gangguan keamanan informasi antara lain:

(a) Mencatat semua rincian penting gangguan dengan segera, seperti jenis pelanggaran, jenis kerusakan, pesan pada layar, atau anomali sistem; dan

(b) Segera melaporkan gangguan ke pihak yang berwenang sebelum melakukan tindakan penanganan secara mandiri.

(4) Sebagai referensi yang digunakan dalam proses penanganan pelanggaran disiplin bagi pegawai dan pihak ketiga dalam melakukan pelanggaran keamanan informasi.

b. Prosedur Pengelolaan Gangguan Keamanan Informasi

Secara detail diatur dalam ketentuan teknis BKN-CSIRT *(Computer Security Incident Response Team)*.

M. PENGENDALIAN KEAMANAN INFORMASI DALAM PENGELOLAAN KELANGSUNGAN KEGIATAN

1. TUJUAN

Keamanan informasi dalam pengelolaan kelangsungan kegiatan bertujuan untuk melindungi sistem informasi, memastikan berlangsungnya kegiatan dan layanan pada saat keadaan darurat, serta memastikan pemulihan yang tepat.

2. RUANG LINGKUP

a. Proses Pengelolaan Kelangsungan Kegiatan;

b. Penilaian Risiko dan Analisis Dampak Bisnis (*Business Impact Analysis/BIA*);

c. Penyusunan dan Penerapan Rencana Kelangsungan Kegiatan (*Business Continuity Plan/BCP*); dan

d. Pengujian, Pemeliharaan, dan Pengkajian Ulan Rencana Kelangsungan Kegiatan.

3. KEBIJAKAN

a. Unit Pemilik Risiko harus mengelola proses kelangsungan kegiatan pada saat keadaan darurat di lingkungan Unit Pemilik Risiko masing-masing.

b. Unit Pemilik Risiko harus mengidentifikasi risiko, dan menganalisis dampak yang diakibatkan pada saat terjadi keadaan darurat untuk menjamin kelangsungan kegiatan.

c. Unit Pemilik Risiko harus menyusun dan menerapkan Rencana Kelangsungan Kegiatan untuk menjaga dan mengembalikan kegiatan operasional dalam jangka waktu yang disepakati dan level yang dibutuhkan.

d. Unit Pemilik Risiko harus memelihara dan memastikan rencana-rencana yang termuat dalam Rencana Kelangsungan Kegiatan masih sesuai, dan mengidentifikasi prioritas untuk kegiatan uji coba.

e. Unit Pemilik Risiko harus melakukan uji coba Rencana Kelangsungan Kegiatan secara berkala untuk memastikan Rencana Kelangsungan Kegiatan dapat dilaksanakan secara efektif.

4. STANDAR

a. Pengelolaan Kelangsungan Kegiatan pada saat Keadaan Darurat Komponen yang harus diperhatikan dalam mengelola proses kelangsungan kegiatan:

1) Identifikasi risiko dan analisis dampak yang diakibatkan pada saat terjadi keadaan darurat;

2) Identifikasi seluruh aset informasi yang menunjang proses kegiatan kritikal;

3) Identifikasi sumber daya, mencakup biaya, struktur organisasi, teknis pelaksanaan, pegawai dan pihak ketiga;

4) Memastikan keselamatan pegawai, dan perlindungan terhadap perangkat pengolah informasi dan aset organisasi;

5) Penyusunan dan pendokumentasian Rencana Kelangsungan Kegiatan sesuai dengan Rencana Strategi (Renstra) Badan Kepegawaian Negara; dan

6) Pelaksanaan uji coba dan pemeliharaan Rencana Kelangsungan Kegiatan secara berkala.

b. Proses identifikasi risiko mengikuti ketentuan mengenai Penerapan Manajemen Risiko di lingkungan BKN.

c. Proses analisis dampak kegiatan harus melibatkan pemilik proses bisnis dan dievaluasi secara berkala.

d. Penyusunan Rencana Kelangsungan Kegiatan mencakup:

1) Proses saat keadaan darurat, mencakup tindakan yang harus dilakukan serta pengaturan hubungan dengan pihak berwenang;

2) Prosedur *fallback*, mencakup tindakan yang harus diambil untuk memindahkan kegiatan kritikal atau layanan pendukung ke lokasi kerja sementara, dan mengembalikan operasional kegiatan kritikal dalam jangka waktu sesuai dengan standar ketersediaan data yang ditetapkan dalam Prosedur Operasional Standar Pengelolaan *Data Center* di BKN;

3) Prosedur saat kondisi telah normal (*resumption*) adalah tindakan mengembalikan kegiatan operasional ke kondisi normal;

4) Jadwal uji coba, mencakup langkah-langkah dan waktu pelaksanaan uji coba serta proses pemeliharaannya;

5) Pelaksanaan pelatihan dan sosialisasi dalam rangka meningkatkan kepedulian dan pemahaman proses kelangsungan kegiatan dan memastikan proses kelangsungan kegiatan dilaksanakan secara efektif;

6) Tanggung jawab dan peran setiap Petugas Pelaksana Pengelolaan Proses Kelangsungan; dan

7) Daftar kebutuhan aset informasi kritikan dan sumber daya untuk dapat menjalankan prosedur saat keadaan darurat, fallback dan saat kondisi telah normal (*resumption*).

e. Uji Coba Rencana Kelangsungan Kegiatan harus dilaksanakan untuk memastikan setiap rencana yang disusun dapat dilakukan/dipenuhi pada saat penerapannya. Kegiatan uji coba Rencana Kelangsungan Kegiatan ini mencakup:

1) Simulasi terutama untuk Petugas Pelaksana Pengelolaan Proses Kelangsungan Kegiatan;

2) Uji coba *recovery* sistem informasi untuk memastikan sistem informasi dapat berfungsi kembali;

3) Uji coba proses *recovery* di lokasi kerja sementara untuk menjalankan proses bisnis secara paralel; dan

4) Uji coba keseluruhan mulai dari organisasi, petugas, peralatan, perangkat, dan prosesnya.

N. PENGENDALIAN KEPATUHAN

1. TUJUAN

Pengendalian kepatuhan bertujuan untuk menghindari pelanggaran terhadap peraturan perundangan yang terkait keamanan informasi.

2. RUANG LINGKUP

a. Kepatuhan terhadap peraturan perundangan yang terkait keamanan informasi;
b. Kepatuhan teknis; dan
c. Audit keamanan SPBE.

3. KEBIJAKAN

a. Kepatuhan Terhadap Peraturan Perundangan yang terkait Keamanan Informasi
   1) Seluruh pegawai dan pihak ketiga harus menaati peraturan perundangan yang terkait dengan keamanan informasi.
   2) Identifikasi peraturan perundangan yang dapat diterapkan Unit TIK harus mengidentifikasi, mendokumentasikan dan memelihara kemutakhiran semua peraturan perundangan yang terkait dengan sistem keamanan informasi.
   3) Hak Atas Kekayaan Intelektual
      Perangkat lunak yang dikelola unit TIK harus mematuhi ketentuan penggunaan lisensi. Penggandaan perangkat lunak secara tidak sah tidak diizinkan dan merupakan bentuk pelanggaran.
   4) Perlindungan terhadap rekaman
      Rekaman milik BKN harus dilindungi dari kehilangan, kerusakan, dan penyalahgunaan.
   5) Pengamanan Data
      Unit Kerja Pemilik Risiko melindungi kepemilikan dan kerahasiaan data. Data hanya digunakan untuk kepentingan yang dibenarkan oleh peraturan perundangan dan kesepakatan.
b. Kepatuhan Teknis
   Unit TIK harus melakukan pemeriksaan kepatuhan teknis secara berkala untuk menjamin efektivitas standar dan prosedur keamanan informasi yang ada di era operasional.

c. Audit Keamanan SPBE

1) Pengendalian audit sistem keamanan SPBE

Tim Auditor harus membuat perencanaan persyaratan, ruang lingkup, dan kegiatan audit yang melibatkan pemeriksaan sistem operasional untuk mengurangi kemungkinan risiko gangguan yang bisa terjadi terhadap kegiatan Badan Kepegawaian Negara selama proses audit.

2) Perlindungan terhadap alat bantu (*tools*) audit sistem informasi

Penggunaan alat bantu (baik perangkat lunak maupun perangkat keras) untuk mengetahui kelemahan keamanan, memindai (*scanning*) kata sandi, atau untuk melemahkan dan menerobos sistem keamanan tidak diizinkan, kecuali atas persetujuan pimpinan unit TIK.

3) Audit sistem informasi di BKN akan ditetapkan dalam ketentuan sendiri.

4. STANDAR

a. Kepatuhan terhadap Hak Kekayaan Intelektual

Hal yang perlu diperhatikan dalam melindungi segala materi yang dapat dianggap kekayaan intelektual meliputi:

1) Mendapatkan perangkat lunak hanya melalui sumber yang dikenal dan memiliki reputasi baik, untuk memastikan hak cipta tidak dilanggar;
2) Memelihara daftar aset informasi sesuai persyaratan untuk melindungi hak kekayaan intelektual;
3) Memelihara bukti kepemilikan lisensi, master disk, buku manual, dan lain sebagainya;
4) Menerapkan pengendalian untuk memastikan jumlah pengguna tidak melampaui lisensi yang dimiliki;
5) Melakukan pemeriksaan bahwa hanya perangkat lunak dan produk berlisensi yang dipasang;
6) Patuh terhadap syarat dan kondisi untuk perangkat lunak dan informasi yang didapat dari jaringan publik;
7) Dilarang melakukan duplikasi, konversi ke format lain atau mengambil dari rekanan komersial (film atau video), selain yang diperbolehkan oleh Undang-Undang Hak Cipta; dan
8) Tidak menyalin secara penuh atau sebagian buku, artikel, laporan, atau dokumen lainnya, selain yang diizinkan oleh Undang-Undang Hak Cipta.

b. Kepatuhan terhadap Kebijakan dan Standar

Hal yang dilakukan jika terdapat kepatuhan teknis meliputi:

1) Menentukan dan mengevaluasi penyebab ketidakpatuhan;
2) Menentukan tindakan yang perlu dilakukan berdasarkan hasil evaluasi agar ketidakpatuhan tidak terulang kembali;
3) Menentukan dan melaksanakan tindakan perbaikan yang sesuai; dan
4) Mengkaji tindakan perbaikan yang dilakukan.

c. Kepatuhan Teknis

Sistem informasi harus diperiksa secara berkala untuk memastikan pengendalian perangkat keras dan perangkat lunak telah diimplementasikan secara benar. Kepatuhan teknis juga mencakup pengujian penetrasi (*penetration testing*) untuk mendeteksi kerentanan dalam sistem, dan memeriksa pengendalian akses untuk mencegah kerentanan tersebut telah diterapkan.

d. Kepatuhan terkait Audit Sistem Informasi

1) Persyaratan audit harus disetujui oleh CIO BKN dan/atau Pimpinan unit kerja setingkat Pimpinan Tinggi Madya;
2) Ruang lingkup pemeriksaan/audit harus disetujui dan dikendalikan oleh pihak berwenang;
3) Pemeriksaan perangkat lunak dan data harus dibatasi untuk akses baca saja (*read-only*);
4) Selain akses baca saja hanya diizinkan untuk salinan dari file sistem yang diisolasi, yang harus dihapus bila audit telah selesai, atau diberikan perlindungan yang tepat jika ada kewajiban untuk menyimpan file tersebut di bawah persyaratan dokumentasi audit;
5) Sumber daya untuk melakukan pemeriksaan harus secara jelas diidentifikasi dan tersedia;
6) Persyaratan untuk pengolahan khusus atau tambahan harus diidentifikasi dan disepakati;
7) Semua akses harus dipantau dan dicatat untuk menghasilkan jejak audit, dan untuk data dan sistem informasi sensitif harus mempertimbangkan pencatatan waktu (*timestamp*) pada jejak audit;
8) Semua prosedur, persyaratan, dan tanggung jawab harus didokumentasikan; dan
9) Auditor harus independen dari kegiatan yang diaudit.

O. PENUTUP

1. Apabila dalam pelaksanaan Keputusan ini dijumpai kesulitan, agar dikonsultasikan kepada Kepala Badan Kepegawaian Negara atau pejabat lain yang ditunjuk untuk mendapatkan penjelasan.
2. Demikian Keputusan ini dibuat untuk dapat dilaksanakan sebaik-baiknya.

Plt. KEPALA
BADAN KEPEGAWAIAN NEGARA,

Ditandatangani Secara Elektronik
HARYOMO DWI PUTRANTO