# DAFTAR ISI

# LEMBAR PENGESAHAN

| | Nama dan Jabatan | Tanda Tangan |
|---|---|---|
| **Disahkan Oleh** | Ditandatangani secara elektronik oleh :<br>Kepala Dinas Komunikasi dan Informatika Kab. Kendal<br><br>**ARDHI PRASETIYO, S.STP., M.M.**<br>Pembina Tingkat I/IV b<br>NIP. 19810925 200012 1 001 | |
| | Ditandatangani secara elektronik oleh :<br>Kepala Bidang Statistik dan Persandian<br><br>**Nursikin, S.Sos.**<br>Pembina IV/a<br>NIP. 19781028 199803 1 002 | |

# LEMBAR PERUBAHAN

| No | Bagian / Halaman | Uraian Perubahan | Revisi Ke | Tanggal Revisi |
|---|---|---|---|---|
| 1 | Semua Halaman | Terbitan Pertama | 00 | 01 Oktober 2025 |
| | | | | |
| | | | | |

# BAB I PENDAHULUAN

## 1. TUJUAN

Pedoman ini bertujuan untuk menjaga keamanan data dan informasi serta untuk menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi dari ancaman atau risiko, maka perlu adanya kebijakan mengenai keamanan informasi pada layanan TI di lingkungan Diskominfo Kab. Kendal.

Sistem Manajemen Keamanan Informasi di Diskominfo Kab. Kendal bertujuan untuk:

1.1. Melindungi aset informasi Dinas Kominfo Kab Kendal dari berbagai bentuk ancaman Keamanan Informasi;

1.2. Mengendalikan risiko dan manfaat informasi melalui perlindungan kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) aset informasi; dan

1.3. Meningkatkan komitmen terhadap pelaksanaan Sistem Manajemen Keamanan Informasi untuk mewujudkan Sistem Manajemen Keamanan Informasi sesuai dengan ketentuan peraturan perundang-undangan.

Sistem Manajemen Keamanan Informasi sebagai pedoman keamanan informasi pada layanan TI di lingkungan Diskominfo Kab. Kendal dilaksanakan oleh pegawai, Mitra Kerja dan Pihak Eksternal yang terkait lainnya

## 2. REFERENSI (DASAR HUKUM)

2.1. ISO/IEC 27001:2022 Persyaratan Sistem Manajemen Keamanan Informasi;

2.2. 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);

2.3. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Tahun 5952);

2.4. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Tahun 6820)

2.5. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara RI Tahun 2018 Nomor 182);

2.6. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);

2.7. 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);

2.8. Peraturan Bupati Kendal No. 57 Tahun 2023 Tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintahan Kabupaten Kendal (Berita Daerah Kabupaten Kendal Tahun 2023 Nomor 57).

## 3. DEFINISI (PENGERTIAN UMUM)

3.1. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah bagian dari keseluruhan sistem manajemen organisasi untuk menetapkan, menerapkan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan Keamanan Informasi yang dibangun dengan pendekatan Risiko untuk mencapai visi dan misi Diskominfo Kab. Kendal.

3.2. Akses adalah tindakan untuk memperoleh aset informasi.

3.3. Teknologi Informasi dan Komunikasi yang selanjutnya disebut TIK adalah segala kegiatan yang terkait dengan pemrosesan, pengelolaan dan penyampaian atau pemindahan informasi antar sarana atau media.

3.4. Backup adalah salinan duplikasi dari data atau keseluruhan data dari tempat penyimpanan data ke dalam tempat penyimpanan yang terpisah.

3.5. *Business Continuity Management* (BCM) adalah mekanisme yang mengatur dan memastikan adanya tindakan yang dilakukan ketika aktivitas teknologi informasi mengalami gangguan / hambatan (bencana) serta memastikan bahwa proses bisnis masih dapat berjalan dan pelayanan tidak terhenti.

3.6. *Business Continuity Plan* (BCP) adalah strategi pemulihan bencana yang dirancang.

3.7. Enkripsi adalah metode pengkodean data agar komputer tidak dapat membaca atau menggunakan data.

3.8. Fasilitas Pengolahan Informasi adalah sebuah sistem, layanan, infrastruktur, atau suatu lokasi fisik yang melakukan pengolahan informasi.

3.9. Hak Akses adalah izin yang diberikan untuk memperoleh Aset Informasi.

3.10. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta, maupun penjelasannya yang dapat dilihat, didengar dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik maupun non-elektronik.

3.11. 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.

3.12. Kriptografi adalah teknik yang mengubah data menjadi berbeda dari aslinya dengan menggunakan algoritma matematika sehingga orang yang tidak mengetahui kuncinya tidak akan dapat membongkar data tersebut.

3.13. Pihak Eksternal adalah pihak selain Personel Diskominfo Kab. Kendal.

3.14. Pihak Ketiga adalah semua unsur di luar pengguna unit TIK Diskominfo Kab. Kendal yang bukan bagian dari Diskominfo Kab. Kendal (seperti: konsultan, penyedia jasa komunikasi, pemasok, dan pemelihara perangkat pengolah informasi), dan Perangkat Daerah lain.

3.15. Risiko adalah kejadian atau kondisi yang dapat menimbulkan dampak negatif atau positif terhadap pencapaian sasaran Diskominfo Kab. Kendal.

3.16. Risiko Keamanan Informasi adalah kejadian atau kondisi yang dapat menimbulkan dampak negatif atau positif terhadap terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) Aset Informasi untuk pencapaian visi dan misi Diskominfo Kab. Kendal.

3.17. Media penyimpanan adalah alat yang dapat dipindahkan (portable) dan dapat dihubungkan ke perangkat komputer serta dapat dilepas kembali tanpa membahayakan data di dalamnya.

3.18. Restore adalah memulihkan salinan data cadangan.

3.19. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.

3.20. Sistem Informasi adalah kesatuan komponen yang terdiri lembaga, sumber daya manusia, perangkat keras, perangkat lunak, substansi data, dan Informasi yang terkait satu sama lain dalam satu mekanisme kerja untuk mengelola data dan informasi.

3.21. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah Sistem Manajemen khusus bagi penyelenggara sistem elektronik pelayanan publik untuk mengelola risiko keamanan informasi dan melindungi data.

3.22. *Remote working* adalah suatu aktivitas yang dilakukan oleh Personel Diskominfo Kab. Kendal untuk melakukan pekerjaan dari suatu tempat di luar gedung Diskominfo Kab. Kendal dan tidak terhubung dengan jaringan internal dengan memanfaatkan teknologi

komunikasi sehingga mendapatkan tingkatan akses yang sama seperti saat bekerja di gedung Diskominfo Kab. Kendal.

3.23. *User Acceptance Test* (UAT) merupakan uji penerimaan Aplikasi yang telah dibangun atau dikembangkan yang dilakukan dengan menugaskan pengembang Aplikasi, pelaksana pengendalian mutu, serta pengguna Aplikasi.

3.24. Aset adalah segala sesuatu yang memiliki nilai untuk Diskominfo Kab. Kendal dan karenanya membutuhkan suatu bentuk perlindungan.

3.25. *Data Center* adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, dan pemulihan data.

3.26. Manajemen Puncak adalah Kepala yang menyelenggarakan urusan pemerintahan.

## 4. RUANG LINGKUP

4.1. SMKI di lingkungan Diskominfo Kab. Kendal mengacu kepada kontrol keamanan standar ISO/IEC 27001:2022.

4.2. Kendali keamanan informasi di lingkungan Diskominfo Kab. Kendal, meliputi domain:

4.2.1. Kendali keamanan informasi aspek organisasi

4.2.2. Kendali keamanan informasi aspek sumber daya manusia;

4.2.3. Kendali keamanan informasi aspek fisik dan lingkungan;

4.2.4. Kendali keamanan informasi aspek teknologi; dan

4.2.5. Penutup.

4.3. Pelaksanaan SMKI dilaksanakan oleh satuan kerja yang ada di Diskominfo Kab. Kendal atau Tim Sistem Manajemen Kemanan Informasi (SMKI) yang dibentuk sesuai dengan peran dan tugas serta wewenang masing-masing untuk mendukung implementasi SMKI dengan ruang lingkup manajemen fasilitas Data Center *(facility management Data Center)*

# BAB II KENDALI KEAMANAN INFORMASI ASPEK ORGANISASI

## 1. KEBIJAKAN UNTUK KEAMANAN INFORMASI

1.1. Dokumen SMKI harus disetujui oleh Kepala Diskominfo Kab. Kendal.

1.2. Dokumen SMKI harus disosialisasikan kepada seluruh pegawai Diskominfo Kab. Kendal.

1.3. Kebijakan untuk keamanan informasi harus dievaluasi paling sedikit sekali dalam setahun untuk menjaga kesesuaian efektivitas penerapannya.

1.4. Apabila dari hasil peninjauan terdapat perubahan maka harus dilakukan pengkinian terhadap dokumen tersebut.

## 2. TUGAS DAN TANGGUNG JAWAB KEAMANAN INFORMASI

2.1. Setiap pegawai Diskominfo Kab. Kendal harus memahami mengenai tanggung jawab terkait proses yang dilakukan dan keamanan informasi yang diterapkan di lingkungan Diskominfo Kab. Kendal untuk melindungi aset yang digunakan.

2.2. Penetapan serta pengalokasian tugas dan tanggung jawab dalam pengelolaan SMKI dan keamanan informasi di Diskominfo Kab. Kendal perlu dilakukan dengan jelas dan sesuai dengan kebutuhan SMKI dan keamanan informasi di Diskominfo Kab. Kendal.

## 3. PEMISAHAN TUGAS DAN TANGGUNG JAWAB

3.1. Tugas dan tanggung jawab dalam pekerjaan kritikal perlu dipisahkan untuk mengurangi risiko adanya unsur ketidaksengajaan dalam penyalahgunaan aset sesuai dengan proses otorisasinya.

3.2. Pemisahan tugas dapat dilakukan dengan memastikan bahwa tidak ada seorangpun yang memiliki kemampuan untuk memodifikasi dan menggunakan aset tanpa otorisasi atau deteksi.

3.3. Dalam hal pemisahan tugas dan tanggung jawab sulit untuk dilakukan, kontrol tambahan perlu dipertimbangkan. Hal ini mencakup namun tidak terbatas pada pengawasan manajemen dan/atau audit trail.

3.4. Proses audit SMKI dan keamanan informasi merupakan suatu proses yang harus memiliki pemisahan tugas dan tanggung jawab yang jelas di mana seorang auditor tidak boleh mengaudit pekerjaannya sendiri.

## 4. TANGGUNG JAWAB MANAJEMEN

4.1. Kepatuhan pegawai terhadap SMKI di lingkungan Diskominfo Kab. Kendal wajib diawasi oleh atasan masing-masing.

4.2. Tanggung jawab atasan adalah untuk memastikan bahwa semua pengguna informasi dan sistem informasi:

4.2.1. Telah memahami dan menerapkan tugas dan tanggung jawabnya dalam sistem keamanan informasi organisasi.

4.2.2. Mematuhi seluruh tugas dan tanggung jawabnya sesuai dengan syarat dan ketentuan pada perjanjian kerjanya dan kebijakan keamanan informasi organisasi.

4.2.3. Memiliki keahlian dan kualifikasi keamanan informasi sesuai dengan tugas dan tanggung jawabnya.

## 5. HUBUNGAN DENGAN PIHAK BERWENANG

5.1. Daftar nomor telepon pihak berwenang seperti Pihak Ketiga penyedia layanan jaringan, polisi, pemadam kebakaran, pihak keamanan gedung, dan lainnya perlu didata untuk menanggulangi gangguan terhadap layanan tersebut.

5.2. Hubungan dengan pihak berwenang yang terkait dengan keamanan informasi perlu dipelihara.

5.3. Kontak tersebut perlu dilakukan apabila terjadi kejadian atau insiden yang perlu dilaporkan kepada pihak berwenang tersebut. Sebagai contoh, apabila terjadi pelanggaran hukum, maka kontak dengan pihak kepolisian perlu dilakukan.

5.4. Dalam hal organisasi mengalami serangan melalui internet, maka Pihak Ketiga, seperti penyedia jasa layanan internet atau operator telekomunikasi perlu dihubungi untuk membantu mengatasi serangan tersebut.

## 6. HUBUNGAN DENGAN SPECIAL INTEREST GROUP

6.1. Forum yang terkait dengan keamanan informasi seperti forum keamanan informasi atau asosiasi profesional keamanan informasi harus diikuti oleh personel administrator sistem dengan tujuan untuk mengetahui informasi terkini terkait dengan keamanan informasi seperti teknologi terkini, ancaman dan risiko baru, dan sebagainya.

6.2. Hubungan dengan *Special Interest Group* perlu dilakukan dengan pertimbangan :

6.2.1. Menambah pengetahuan mengenai best practice dan tetap mengikuti perkembangan teknologi dan informasi yang terkait dengan keamanan informasi;

6.2.2. Mendapatkan informasi akan kondisi keamanan informasi terkini;

6.2.3. Mendapatkan informasi secara dini mengenai peringatan, informasi, saran, update atau patch yang terkait dengan keamanan informasi; dan

6.2.4. Pertukaran informasi akan teknologi, produk, ancaman atau kerentanan terbaru yang terkait dengan keamanan informasi.

## 7. THREAT INTELLIGENCE

7.1. *Threat intelligence* berfokus pada pengumpulan, analisis, dan penggunaan informasi untuk melindungi Diskominfo Kab. Kendal dari ancaman keamanan dan menjadi lebih responsif terhadap serangan yang berpotensi merugikan dan meminimalkan dampak negatifnya.

7.2. 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*

7.3. *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.

7.4. Informasi *threat intelligence* yang relevan dikomunikasikan kepada pemangku kepentingan dalam Diskominfo Kab. Kendal 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.

7.5. Tindakan yang diambil dalam merespons ancaman yang terdeteksi melibatkan kegiatan pemantauan terus, pelaporan insiden keamanan, serta prosedur respon insiden dan keberlangsungan bisnis.

## 8. KEAMANAN INFORMASI DALAM MANAJEMEN PROYEK

8.1. Setiap pelaksanaan proyek atau pekerjaan di lingkungan Diskominfo Kab. Kendal perlu diatur mengenai aspek keamanan informasi sebagai bagian dari perjanjian dan pelaksanaan proyek.

8.2. Diskominfo Kab. Kendal harus melakukan *risk assessment* keamanan informasi pada fase awal pelaksanaan proyek/kegiatan untuk mengidentifikasi:

8.2.1. Risiko keamanan informasi yang relevan dalam pelaksanaan proyek; dan

8.2.2. Kontrol keamanan informasi terkait dengan risiko yang teridentifikasi.

8.2.3. Kontrol keamanan informasi yang telah teridentifikasi harus diimplementasikan selama proyek berlangsung, dan apabila diperlukan

setelah proyek berlangsung.

## 9. INVENTARISASI ASET

9.1. Semua aset TIK yang digunakan di lingkungan Diskominfo Kab. Kendal harus diidentifikasikan dan diinventarisasi yang meliputi:

9.1.1. Informasi, yang dikelola di Diskominfo Kab. Kendal.

9.1.2. Perangkat lunak dan aplikasi.

9.1.3. Aset fisik yang meliputi PC, notebook, server, removable media, printer, dan scanner, dan untuk mesin fotokopi.

9.1.4. Perangkat jaringan, layanan jaringan, dan keamanan jaringan.

9.1.5. Sarana maupun layanan pendukung seperti, genset, UPS, dan AC.

9.1.6. Sumber daya manusia.

9.1.7. Layanan Pihak Ketiga.

9.2. Daftar inventarisasi aset TIK tersebut harus diperiksa kesesuaian dan dilakukan pengkinian setiap ada perubahan yang terjadi.

9.3. Metode maupun tingkat pengamanan terhadap aset tersebut perlu ditentukan berdasarkan klasifikasi dari aset tersebut.

9.4. Setiap aset TIK yang digunakan di lingkungan Diskominfo Kab. Kendal harus ditentukan penanggung jawab sebagai bagian pengelolaan aset tersebut, untuk:

9.4.1. Memastikan informasi dan aset informasi telah diklasifikasikan dan diamankan dengan baik.

9.4.2. Menentukan hak akses ke aset tersebut.

9.4.3. Secara periodik melakukan peninjauan terhadap klasifikasi dan pengamanan aset tersebut.

## 10. PENGGUNAAN ASET YANG DITERIMA

10.1. Penggunaan perangkat TIK hanya untuk kepentingan pekerjaan dan merupakan perangkat milik Diskominfo Kab. Kendal

10.2. Apabila ada penggunaan perangkat pribadi yang mengakses ke sistem layanan jaringan Diskominfo Kab. Kendal maka harus meminta persetujuan kepada Pejabat terkait di Diskominfo Kab. Kendal

10.3. Akses ke layanan Jaringan bagi pegawai Diskominfo Kab. Kendal harus ditetapkan aturan dalam penggunaan layanan tersebut untuk menghindari penyalahgunaan akses ke jaringan.

10.4. Aturan mengenai penggunaan informasi dan aset pemrosesan informasi harus dibuat, didokumentasikan dan diimplementasikan.

10.5. Semua pengguna baik pegawai Diskominfo Kab. Kendal maupun Pihak Ketiga harus mematuhi peraturan yang telah dibuat. Peraturan tersebut mencakup namun tidak terbatas pada:

10.5.1. Aturan mengenai *e-mail* dan penggunaan internet; dan

10.5.2. Pedoman untuk penggunaan *mobile device*, khususnya penggunaan device di luar lingkungan kantor.

10.6. Seluruh pegawai Diskominfo Kab. Kendal maupun Pihak Ketiga harus memiliki kesadaran (*awareness*) mengenai aturan penggunaan aset dan tanggung jawab keamanan informasi terkait dengan penggunaan aset tersebut.

10.7. Penanganan terhadap aset harus mengacu kepada keterkaitan dengan klasifikasi jenis aset informasi yang dikelola pada aset tersebut.

10.8. Penanganan aset diperlukan untuk melindungi informasi pada aset tersebut dari kegagalan terhadap aspek kerahasiaan, integritas dan ketersediaan.

10.9. Pemeliharaan informasi atau aset dapat didelegasikan kepada pengelola (*custodian*) dari aset, namun tanggung jawab akhir dari informasi atau aset tersebut tetap terletak pada pemilik informasi atau aset tersebut.

## 11. PENGEMBALIAN ASET

11.1. Setiap pegawai yang sudah tidak berkerja di lingkungan Diskominfo Kab. Kendal harus mengembalikan aset TIK dan informasi milik Diskominfo Kab. Kendal yang sudah bukan menjadi kewenangannya.

11.2. Aset yang dimaksud mencakup seluruh informasi, perangkat keras dan lunak pengolahan informasi.

11.3. Pengembalian aset TIK dilakukan secara formal dan terdokumentasi sesuai dengan ketentuan yang berlaku.

## 12. KLASIFIKASI INFORMASI

12.1. Informasi harus diklasifikasikan sesuai dengan sensitivitas dan kritikalitas informasi tersebut bagi organisasi.

12.2. Klasifikasi informasi merupakan acuan untuk penanganan dan pengamanan informasi organisasi.

12.3. Pembagian tingkat klasifikasi dan penanganan informasi harus mempertimbangkan aspek kerahasiaan, integritas dan ketersediaan informasi.

12.4. Klasifikasi informasi di Diskominfo Kab. Kendal sesuai dengan kebutuhan dan dampak bisnis yang meliputi:

12.4.1. Data Sangat Rahasia adalah aset informasi yang bersifat strategis bagi

organisasi dan berisiko sangat tinggi yang pembocoran atau akses tanpa izin terhadapnya mempunyai konsekuensi hukum. Informasi ini hanya dapat diakses secara sangat terbatas oleh pihak ketiga dan hanya dapat digunakan untuk kepentingan atau karena kewajiban dan kebutuhan organisasi, dengan syarat pihak ketiga dan pegawai pihak ketiga menandatangani Kesepakatan Kewajiban Menjaga Rahasia / *Non-Disclosure Agreement* (NDA). Contoh aset informasi sangat rahasia: Data *Biometrik*.

12.4.2. Data rahasia adalah aset informasi yang sangat peka dan berisiko tinggi atau yang menurut peraturan perundang-undangan dinyatakan rahasia yang pembocoran atau penyalahgunaan akses terhadapnya dapat mengganggu kelancaran kegiatan organisasi atau mengganggu citra dan reputasi organisasi. Informasi ini hanya dapat diakses secara terbatas oleh pihak ketiga dan hanya dapat digunakan untuk kepentingan atau karena kewajiban dan kebutuhan organisasi melalui serah terima resmi dengan syarat pihak ketiga dan pegawai pihak ketiga menandatangani Kesepakatan Kewajiban Menjaga Rahasia / *Non-Disclosure Agreement*. Contoh aset informasi rahasia : IP address, password komputer, insiden siber, analisa insiden siber, hasil *vulnerability assessment-penetration testing*, hasil *assessment* Keamanan infformasi, hasil audit TIK, aduan publik, bahan / materi pelatihan, rencana anggaran/pengadaan, data gaji dan penilaian kinerja pegawai, serta data kesehatan pribadi pegawai yang secara legal harus dilindungi.

12.4.3. Data terbatas adalah aset informasi yang telah terdistribusi secara luas di lingkungan internal organisasi yang penyebarannya secara internal tidak lagi memerlukan izin dari Pemilik Aset Informasi dan risiko penyebarannya oleh pihak yang tidak berwenang tidak menimbulkan kerugian yang berarti. Informasi ini dapat diberikan kepada pihak ketiga oleh pemiliknya untuk kepentingan dinas melalui prosedur serah terima resmi. Contoh aset informasi terbatas: pedoman organisasi, panduan kerja, tata cara kerja, instruksi kerja, memo / publikasi internal, informasi yang disediakan dalam intranet, dan data operasional IT lainnya.

12.4.4. Data internal adalah aset informasi milik dan/atau berhubungan dengan organisasi, dimana hanya pegawai yang bekerja pada organisasi saja yang dapat mengakses data internal.

12.4.5. Data publik adalah aset informasi yang secara sengaja disediakan oleh organisasi untuk dapat diketahui masyarakat umum. Contoh aset informasi publik : brosur, situs publik organisasi, dan siaran pers (*press release*).

12.5. Klasifikasi informasi juga harus mempertimbangkan kebutuhan layanan informasi dan pelaksanaan tugas dan fungsi Kementerian serta dampak terhadap bisnis apabila terjadi kegagalan keamanan.

12.6. Perlindungan terhadap aset informasi yang bersifat rahasia harus disesuaikan dengan tingkat keamanan yang memadai sesuai dengan aturan penanganan informasi yang diterapkan di Diskominfo Kab. Kendal

12.7. Pemilik informasi selaku pemilik proses bisnis sesuai dengan ketentuan peraturan perundang-undangan bertanggung jawab untuk :

12.7.1. Mengklasifikasikan informasi yang dimilikinya; dan

12.7.2. Peninjauan secara periodik terhadap klasifikasi informasi untuk memastikan bahwa klasifikasi telah sesuai dengan kondisi dan kebutuhan terkini organisasi (*up to date*).

12.8. Pemilik informasi wajib menyusun dokumen pedoman klasifikasi informasi.

## 13. PELABELAN DAN PENANGANAN INFORMASI

13.1. Prosedur terkait dengan pelabelan dan penanganan informasi harus dikembangkan dan diimplementasikan berdasarkan sistem klasifikasi informasi organisasi.

13.2. Penanganan informasi khususnya yang bersifat rahasia mencakup pada aspek pemrosesan, penyimpanan, distribusi, dan pemusnahan informasi harus diterapkan secara aman.

13.3. Prosedur pelabelan informasi harus mencakup segala bentuk informasi baik *hardcopy* maupun *softcopy*.

13.4. Informasi yang bersifat *hardcopy* harus diberi kode (label) untuk memastikan penanganan informasi sesuai dengan tingkat klasifikasinya.

13.5. Data / informasi yang tersimpan dalam media elektronik (*softcopy*) harus mendapatkan perlakukan sesuai kerahasiaannya dan diusahakan diberikan *password* atau pembatasan akses ke folder.

13.6. Prosedur penanganan informasi, yang mencakup proses penyimpanan, transfer dan pemusnahan harus didefinisikan dengan jelas untuk setiap kategori klasifikasi.

## 14. PERTUKARAN INFORMASI

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

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

14.2.1. Pengamanan pertukaran informasi dari ancaman *interception, copying*, modifikasi, *misrouting*, dan pengrusakan.

14.2.2. Perlindungan informasi dari malware yang dapat ditransmisikan melalui penggunaan media komunikasi elektronik.

14.2.3. Mengatur tata cara penggunaan media komunikasi elektronik seperti e-mail dan internet.

14.2.4. Pengamanan media komunikasi wireless secara aman.

14.2.5. Diskominfo Kab. Kendal harus memiliki kebijakan dan pedoman terkait dengan *acceptable use of electronic communication*.

14.2.6. Pemberian *awareness* kepada semua pegawai untuk bertanggung jawab dalam bertukar informasi sehingga tidak menyebabkan berkurangnya reputasi organisasi, seperti melakukan pencemaran nama baik, *impersonation*, pelecehan atau pengiriman surat kaleng.

14.2.7. Kriptografi harus digunakan untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi yang dipertukarkan.

14.2.8. Informasi sensitif tidak boleh ditinggalkan pada fasilitas pencetakan seperti mesin photocopy, printer, mesin fax tanpa pengawasan.

14.2.9. Kontrol harus diterapkan untuk mengatur atau melarang *automatic forwarding* dalam penggunaan layanan informasi, seperti *automatic e-mail forwarding* dari e-mail organisasi ke e-mail pribadi.

14.2.10. Pemberian *awareness* agar pegawai berhati-hati apabila berkomunikasi di ruang publik.

14.2.11. Tidak meninggalkan informasi sensitif pada *answering machine*.

14.2.12. Menjaga prinsip kehati-hatian dalam menggunakan mesin faximile.

14.2.13. Pembatasan atau larangan untuk memberikan data pribadi seperti alamat e-mail atau data pribadi lainnya yang mungkin dapat disalahgunakan oleh pihak luar.

14.2.14. Cache pada printer dan mesin photocopy harus dipastikan terhapus.

14.2.15. Personel tidak diperbolehkan melakukan percakapan mengenai informasi rahasia organisasi pada tempat umum.

14.3. Diskominfo Kab. Kendal dalam melaksanakan pertukaran data dan informasi harus memastikan adanya perjanjian formal dalam melakukan pertukaran informasi dengan pihak lain untuk memastikan semua pihak yang terlibat melakukan pengamanan informasi dengan memuat hal-hal sebagai berikut:

14.3.1. Kesepakatan dalam kesepahaman yang sama terkait keamanan informasi sehingga informasi dapat dilindungi secara memadai.

14.3.2. Penyimpanan informasi secara aman dan memadai.

14.3.3. Penggunaan sistem pelabelan yang telah disepakati untuk informasi yang sensitif serta memastikan bahwa sistem tersebut dapat dengan mudah dimengerti.

14.3.4. Penggunaan teknologi *password* yang diperlukan.

14.4. Kesepakatan atau perjanjian tersebut perlu mempertimbangkan beberapa aspek keamanan berikut :

14.4.1. Tanggung jawab manajemen dalam melakukan pengendalian dan notifikasi transmisi informasi, *dispatch*, dan penerimaan informasi.

14.4.2. Standar teknis dalam pengemasan dan transmisi.

14.4.3. Perjanjian *escrow*, merupakan perjanjian yang mengatur lisensi dan *source code* dari software dengan Pihak Ketiga penyedia software tersebut.

14.4.4. Pengunaan kurir yang aman.

14.4.5. Tugas dan tanggung jawab pada saat terjadinya insiden keamanan informasi seperti kehilangan data.

14.4.6. Kepemilikan dan tanggung jawab untuk perlindungan data, copyright dan kepatuhan pada hukum lisensi.

14.4.7. Penggunaan teknologi kriptografi.

14.5. Pengiriman informasi milik Diskominfo Kab. Kendal menggunakan metode pesan elektronik, seperti e-mail, chat, *file sharing*, *cloud storage* harus dilindungi untuk menghindari kebocoran informasi secara tidak disengaja akibat kesalahan pengiriman dan tanpa ada pengamanan pada file.

14.6. Perlindungan tersebut perlu mempertimbangkan aspek-aspek berikut:

14.6.1. *Awareness* kepada pengguna untuk memastikan keamanan dalam penggunaan fasilitas pesan elektronik;

14.6.2. Mengamankan informasi yang dikirimkan menggunakan media pesan elektronik sesuai dengan klasifikasi informasi tersebut;

14.6.3. Penggunaan teknologi kriptografi untuk menjaga kerahasiaan dan integritas dari informasi yang dikirimkan serta untuk memastikan identitas dari partner pengiriman informasi tersebut;

14.6.4. Membatasi penggunaan layanan pesan elektronik yang bersifat publik dalam mengirim informasi.

14.7. Setiap pegawai yang aktif di Diskominfo Kab. Kendal berhak mendapatkan alamat e-mail untuk keperluan komunikasi dan kolaborasi untuk melaksanakan tugas yang berkaitan dengan organisasi.

14.8. *E-mail* hanya digunakan untuk tujuan bisnis, operasional, dan kepentingan layanan

organisasi.

14.9. Penggunaan *e-mail* tidak diperbolehkan untuk kegiatan-kegiatan berikut:

14.9.1. Pembahasan hal yang berkaitan dengan kegiatan politik atau isu politik.

14.9.2. 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 kelas sosial.

14.9.3. Pengiriman pesan yang berasal dari sumber yang tidak dapat dipertanggungjawabkan kebenarannya, seperti surat kaleng.

14.9.4. Mengirim pesan untuk keuntungan pribadi.

14.9.5. Mengambil dan mengirim pesan dalam sebuah file yang tidak terkait dengan kepentingan organisasi.

14.9.6. Penyebaran informasi ke sistem e-mail pengguna untuk hal-hal yang tidak berhubungan dengan kegiatan organisasi.

14.10. Daftar penerima (*To, Cc*, dan *Bcc*), *subject*, lampiran dan/atau konten *e-mail* sepenuhnya menjadi tanggung jawab pengirim.

14.11. Tidak boleh membuka atau mengirimkan e-mail yang tidak diketahui dan/atau diduga / dianggap virus / spam / junk e-mail kepada pengguna e-mail lain. Bila menemukan hal tersebut segera menghapus e-mail tersebut.

14.12. Jika mengirimkan atau menerima lampiran file harus melakukan scanning.

14.13. Jika mengirimkan lampiran file yang besar diharuskan untuk mengkompresi lampiran file sebelum dikirimkan.

14.14. Untuk menjaga keandalan dan ketersediaan layanan e-mail, beberapa jenis file tidak diperbolehkan untuk dimasukan sebagai lampiran *e-mail* (misalnya: bat., cmd., *file* multimedia, dan lain- lain).

14.15. Dalam penulisan *disclaimer* untuk *e-mail* yang akan dikirimkan, perlu mencakup beberapa hal sebagai berikut:

14.15.1. *Disclaimer* harus mencantumkan klausul mengenai keamanan informasi.

14.15.2. *Disclaimer* harus menginformasikan bahwa informasi yang terkandung dalam e-mail adalah milik organisasi.

14.15.3. *Disclaimer* harus mencantumkan klausul mengenai langkah yang harus dilakukan apabila penerima e-mail bukanlah sebagaimana yang dimaksud oleh pengirim.

14.15.4. *Disclaimer* mencantumkan pelarangan mengenai pembacaan, pendistribusian dan duplikasi informasi yang terkandung pada e-mail yang bukan haknya (penerima e-mail bukanlah sebagaimana yang dimaksud oleh

pengirim)

14.16. Setiap e-mail yang tersimpan dalam kotak masuk e-mail memiliki masa aktif. Penyedia layanan tidak bertanggung jawab atas segala sesuatu yang berkaitan dengan penghapusan e-mail.

14.17. Setiap mengirim e-mail (*send*), mengirim balik (*reply*) atau meneruskan (*forward*) harus mencantumkan nama pengirim dan *subject* diisi harus mencerminkan isi e-mail, serta format penulisan isi mengikuti ketentuan penulisan surat dinas organisasi.

14.18. Apabila mengirim balik (*reply*) atau meneruskan (*forward*) e-mail tidak diperbolehkan untuk mengubah, mengurangi maupun menambah pada e-mail aslinya.

14.19. Tidak diperbolehkan mengirim (*send*), mengirim balik (*reply*), meneruskan/menyebarkan (*forward*) suatu e-mail berantai, iklan, *spam*, *phising*, *bulk*, *hoax* atau e-mail yang berisi *virus, worm, trojan, spyware, rootkit* atau program jahat lain.

14.20. Tidak diperbolehkan mengirim balik ke semua (*reply all*) jika materi e-mail yang dikirim tidak berhubungan langsung dengan *all recipient*.

14.21. Semua e-mail yang dibuat, disimpan, dikirim atau diterima pegawai melalui sistem e-mail adalah milik organisasi.

14.22. Diskominfo Kab. Kendal berhak melakukan pengecekan atau membuka e-mail yang keluar atau masuk ke dalam sistem tanpa pemberitahuan sebelumnya.

14.23. Diskominfo Kab. Kendal berhak untuk mengumpulkan, menyimpan, menggunakan atau mengungkapkan informasi pribadi, dalam rangka penyelidikan atau penegakan hukum, dan hanya dapat diajukan oleh unit Internal Audit atau Kepala Diskominfo Kab. Kendal

14.24. E-mail digunakan untuk surat resmi organisasi, komunikasi pekerjaan dan untuk mendistribusikan buletin/berita yang berhubungan dengan pekerjaan.

## 15. KETENTUAN PENGENDALIAN HAK AKSES

15.1. Akses terhadap Informasi harus sesuai dengan kewenangan yang dimiliki dan User ID yang unik.

15.2. Setiap pengguna yang dapat mengakses sistem wajib menggunakan User ID dan password-nya masing-masing.

15.3. Standardisasi profil akses misalnya berupa hak akses administrator, dan pengguna pada setiap sistem perlu ditetapkan.

15.4. Mekanisme untuk kegiatan pengajuan hak akses, otorisasi hak akses, pengadministrasian hak akses, pemantauan hak akses perlu dilakukan secara periodik.

15.5. Setiap pemilik informasi dan aset pemrosesan informasi bertanggung jawab untuk penyusunan kebijakan pengendalian hak akses tersebut.

15.6. Kebijakan tersebut dapat diwujudkan dengan penyusunan sebuah matriks hak akses untuk memetakan pengguna dengan hak akses dan informasi atau aset pengolahan informasi.

15.7. Pengguna hanya akan diberikan akses ke informasi atau aset informasi organisasi berdasarkan kebutuhan operasional pekerjaannya.

15.8. Fitur keamanan, tingkat layanan dan kebutuhan terhadap layanan jaringan yang diidentifikasi dalam operasional sistem di Diskominfo Kab. Kendal harus dimonitor dan dievaluasi secara berkala.

15.9. Perangkat milik pribadi tidak diperkenankan terhubung ke jaringan internal Diskominfo Kab. Kendal

15.10. Semua akses ke perangkat layanan jaringan Diskominfo Kab. Kendal hanya dapat dilakukan oleh pegawai penanggung jawab jaringan yang telah mendapatkan otorisasi dari Koordinator Manajemen Fisik dan Sistem Informasi.

15.11. Akses jaringan melalui *remote* harus mendapatkan persetujuan dari Koordinator Manajemen Fisik dan Sistem Informasi.

15.12. Penggunaan jaringan harus direviu berkala melalui audit log yang dilakukan untuk mengidentifikasi kejadian atau kelemahan yang dapat menimbulkan kegagalan keamanan (*security breach*).

15.13. Fitur keamanan layanan jaringan di Diskominfo Kab. Kendal sedapat mungkin telah menerapkan teknologi pengamanan jaringan, seperti otentifikasi dan enkripsi jaringan.

15.14. Pengguna (*user*) hanya diperbolehkan untuk mengakses jaringan dan layanan jaringan yang diizinkan sesuai area kerjanya.

15.15. Pemberian akses ke jaringan dan layanan jaringan organisasi harus berdasarkan kebutuhan operasional pekerjaan pengguna yang bersangkutan.

15.16. Perhatian lebih dan pengamanan tambahan harus diberikan untuk akses ke jaringan dan layanan jaringan internal organisasi dari jaringan internet (*remote access*).

## 16. PENDAFTARAN PENGGUNA (USER) DAN PENGHAPUSAN HAK AKSES

16.1. Diskominfo Kab. Kendal harus menerapkan proses registrasi dan deregistrasi user untuk perizinan akses ke dalam sistem informasi dan jaringan.

16.2. Pemberian hak akses pengguna harus dilengkapi dengan otentikasi dan otorisasi serta harus diadministrasikan.

16.3. Penggunaan User ID harus bersifat unik dan harus menunjukkan identitas nama dengan jelas bagi setiap Pengguna dan telah mendapatkan persetujuan dari Pimpinan

Unit.

16.4. Memastikan bahwa tingkat hak akses yang diberikan kepada pengguna telah sesuai dengan kewenangannya.

16.5. Segera mencabut atau menonaktifkan User ID dan hak akses bagi pegawai Diskominfo Kab. Kendal yang telah berganti fungsi, tugas atau telah meninggalkan lingkungan Diskominfo Kab. Kendal

16.6. Menghindari penggunaan User ID secara bersama (*shared*) kecuali untuk kondisi di mana penggunaan tersebut memiliki justifikasi operasional dan bisnis. Penggunaan User ID harus disetujui secara formal dan didokumentasikan.

## 17. PENGOLAAN INFORMASI OTENTIFIKASI

17.1. Semua user harus memiliki User ID dan hanya untuk digunakan secara individu.

17.2. Penggunaan User ID secara bersama (*shared*) harus dibatasi dan hanya untuk kondisi dimana perangkat atau sistem yang dijalankan tidak memungkinkan pemisahan User ID.

17.3. Informasi otentikasi rahasia adalah informasi rahasia yang digunakan untuk mengotentikasikan seorang pengguna pada saat akan mengakses sebuah sistem informasi. Contoh dari informasi ini mencakup namun tidak terbatas pada *password, smartcard*, token, atau PIN.

17.4. Pemberian informasi otentifikasi rahasia harus dikendalikan melalui proses pengelolaan formal.

17.5. Pengelolaan informasi otentifikasi rahasia perlu memastikan:

17.5.1. Pengguna (*user*) memahami tanggung jawabnya untuk menjaga keamanan dari informasi otentifikasi yang dimilikinya.

17.5.2. Untuk informasi otentifikasi dalam bentuk *password*, apabila pengguna terpaksa memberikan *password* tersebut kepada pihak lain. Maka, pengguna harus mengganti informasi tersebut pada kesempatan pertama.

17.5.3. Pengguna dilarang memberikan informasi otentifikasi rahasia miliknya kepada pihak lain.

17.5.4. *Password* sementara yang tidak mudah ditebak dapat diberikan kepada pengguna untuk melakukan akses untuk pertama kali ke sistem informasi organisasi. Pengguna harus segera mengganti *password* sementara tersebut.

17.5.5. Penyimpanan informasi otentifikasi harus dilakukan secara aman dengan perlindungan yang tepat.

17.5.6. Informasi otentifikasi yang bersifat *default* dari vendor harus diganti setelah

dilakukan instalasi sistem atau perangkat lunak.

17.6. Setiap Pegawai di lingkungan Diskominfo Kab. Kendal wajib menggunakan *password* di perangkat yang digunakan dan menjaga kerahasiaan *password* dan menghindari menyimpan catatan *password* di tempat terbuka.

17.7. Setiap Pegawai di lingkungan Diskominfo Kab. Kendal wajib mengganti *password* apabila ada indikasi sistem dan *password* mengalami penyalahgunaan atau kebocoran.

17.8. Penggunaan *password* harus yang berkualitas yang meliputi:

17.8.1. Panjang minimal karakter *password* pada sistem dan perangkat yang digunakan adalah 8 (delapan);

17.8.2. Menggunakan kombinasi huruf dan angka, sedapat mungkin menggunakan spesial karakter (seperti: !$%#*) kecuali apabila sistem atau aplikasi tidak memungkinkan.

17.8.3. Untuk sistem yang tidak dimungkinkan mengikuti penggunaan *password* yang berkualitas harus mendapatkan persetujuan dari Kepala Diskominfo Kab. Kendal dengan mempertimbangkan kendala dan risiko yang ada.

17.9. *Password* tidak boleh sama dengan User ID dan tidak berdasar pada sesuatu yang mudah ditebak misalnya: nama, nomor telepon, tanggal lahir, nama anggota keluarga, nama/identitas organisasi.

17.10. Mengganti *password* secara reguler selama 3 (tiga) bulan dengan menghindari menggunakan *password* yang sudah pernah digunakan.

17.11. Setiap pengguna wajib menjaga kerahasiaan *password* dan tidak diperkenankan memberikan *password*-nya kepada orang lain dan/atau menggunakan *password* milik orang lain.

17.12. Pengguna diwajibkan untuk mengikuti kebijakan dan prosedur yang berlaku dalam pemilihan dan penggunaan informasi otentikasi rahasia.

17.13. Informasi otentikasi rahasia adalah informasi rahasia yang digunakan untuk mengotentikasikan seorang pengguna pada saat akan mengakses sebuah sistem informasi. Contoh dari informasi ini mencakup namun tidak terbatas pada *password*, *smartcard*, token, atau PIN.

17.14. Terkait dengan keamanan informasi otentifikasi rahasia, pengguna (*user*) sistem informasi perlu memastikan:

17.14.1. Tidak terdiri dari urutan karakter baik angka, huruf maupun lokasi pada keyboard, seperti 12345678, asdfgh atau 1234zxcv.

17.14.2. Mengganti *password* sementara pada saat pertama kali log-on.

17.14.3. Tidak menggunakan atau memasukkan *password* ke sistem secara otomatis.

17.14.4. Tidak menggunakan *password* yang sama untuk penggunaan bisnis dan pribadi.

17.14.5. Untuk penggunaan informasi rahasia yang bersifat *password* beberapa hal berikut harus dijalankan :

- Menggunakan *password* yang mudah diingat, namun tidak mudah ditebak.
- Tidak terdiri dari urutan karakter baik angka, huruf maupun lokasi pada *keyboard*, seperti 12345678, asdfgh atau 1234zxcv.
- Mengganti *password* sementara pada saat pertama kali *log-on*.
- Tidak menampilkan karakter *password* pada saat *log-on*.
- Tampilan karakter *password* dapat diganti dengan simbol.

17.1. Administrator pengelola sistem informasi perlu memperhatikan dengan seksama dan mencatat setiap laporan kehilangan informasi otentikasi rahasia atau permintaan *reset password*.

17.2. Sistem manajemen *password* harus memastikan penggantian *password* secara reguler yaitu maksimal 3 (tiga) bulan sekali.

17.3. Sistem untuk mengelola *password* perlu menggunakan sistem yang interaktif dan harus dapat memastikan kualitas *password* pengguna sistem informasi organisasi.

17.4. Sistem manajemen *password* harus memastikan:

17.4.1. Penggunaan User ID dan *password* individual untuk setiap pegawai.

17.4.2. Pengguna dapat mengganti *password*-nya.

17.4.3. Memastikan penggunaan *password* yang sesuai dengan aturan terkait penggunaan *password*.

17.4.4. Memastikan pengguna mengganti *password* sementara pada saat *log-on* untuk pertama kali.

17.4.5. Tidak menampikan *password*.

17.4.6. Menyimpan file yang berisi *password* secara terpisah dari data aplikasi.

17.4.7. Penyimpanan dan pengiriman *password* harus menggunakan perlindungan khusus seperti enkripsi dan *hashing.*

## 18. HAK AKSES

18.1. Proses pengadaan untuk memberikan atau mencabut hak akses yang diberikan kepada *User* ID meliputi:

18.1.1. Memperoleh otorisasi dari pimpinan masing-masing unit kerja pada Diskominfo Kab. Kendal;

18.1.2. Memverifikasi bahwa tingkat akses yang diberikan adalah sesuai dengan kebijakan akses;

18.1.3. User yang telah rotasi/mutasi/demosi/promosi segera hak aksesnya disesuaikan dengan posisinya;

18.1.4. User yang telah pensiun segera hak aksesnya dihapus atau diblokir; dan

18.1.5. Melakukan *review* pemberian hak akses secara berkala.

18.2. Permintaan hak akses harus diajukan secara formal oleh atasan langsung dari pemohon hak akses dan disetujui oleh pemilik dan administrator yang berwenang untuk sistem tersebut.

18.3. Persetujuan pemberian hak akses perlu memperhatikan kebutuhan operasional pekerjaan.

18.4. Pemberian hak akses harus di-review secara berkala untuk mengidentifikasi perubahan terhadap pengguna seperti promosi, demosi, perpindahan posisi atau terminasi kepegawaian.

18.5. Seluruh proses pemberian dari hak akses tersebut harus didokumentasikan dengan baik.

18.6. Administrator sistem di Diskominfo Kab. Kendal harus melakukan peninjauan terhadap hak akses user secara berkala.

18.7. Peninjauan dilakukan secara reguler, sekali setiap 6 (enam) bulan dan setiap ada perubahan terhadap pengguna.

18.8. Otorisasi untuk hak akses khusus (*privileged*) harus ditinjau secara reguler dengan jangka waktu setiap 3 (tiga) bulan, dibanding dengan peninjauan hak akses biasa.

18.9. Peninjauan ini merupakan tanggung jawab dari pemilik informasi dan/atau sistem informasi terkait.

18.10. Perubahan pada hak akses khusus perlu didokumentasikan.

18.11. Pencabutan atau penyesuaian hak akses dari pegawai Diskominfo Kab. Kendal harus dihapus atau diblok untuk menentukan apakah perlu untuk penghapusan hak akses setelah pemutusan hubungan kerja mereka, atau disesuaikan jika ada perubahan.

18.12. Beberapa saat sebelum proses pemberhentian atau pergantian status kepegawaian perlu dipertimbangkan untuk membatasi akses kepada informasi atau sistem informasi organisasi.

18.13. Prosedur terkait penghapusan hak akses diatur dalam dokumen pengelolaan hak akses.

## 19. KEAMANAN INFORMASI UNTUK PIHAK KETIGA

19.1. Proses keamanan informasi dengan Pihak Ketiga harus disepakati dengan Pihak

Ketiga terkait dengan akses Pihak Ketiga untuk aset organisasi

19.2. Setiap Pihak Ketiga Diskominfo Kab. Kendal harus diidentifikasi dan didokumentasikan. Dokumentasi harus mencakup informasi terkait Pihak Ketiga, layanan yang diberikan serta referensi ke kontrak kerja.

19.3. Pemilihan dari Pihak Ketiga harus mengikuti kriteria berikut:

19.3.1. Kompetensi, pengalaman dan catatan dari organisasi;

19.3.2. Kepastian dari kemampuan Pihak Ketiga untuk menyediakan layanan;

19.3.3. Kepastian dari kemampuan Pihak Ketiga untuk menjaga ketersediaan dari penyediaan layanan pada saat kondisi normal atau kondisi bencana (apabila terjadi bencana alam atau kegagalan dalam penyediaan layanan).

19.4. Setiap kontrak kerja antara organisasi dan Pihak Ketiga harus mencakup:

19.4.1. Perjanjian kerahasiaan;

19.4.2. Prasyarat untuk mengikuti persyaratan keamanan informasi Diskominfo Kab. Kendal;

19.4.3. Tanggung jawab dari kedua belah pihak; dan

19.4.4. Jika penyediaan layanan oleh Pihak Ketiga melibatkan subkontraktor, Pihak Ketiga harus menyediakan kepastian bahwa persyaratan keamanan informasi Diskominfo Kab. Kendal akan diikuti oleh para subkontraktor.

19.5. Akses ke informasi dan aset data center pada Diskominfo Kab. Kendal yang dilakukan oleh Pihak Ketiga harus diberikan berdasarkan kebutuhan dan disetujui oleh Diskominfo Kab. Kendal

19.6. Personel Pihak Ketiga harus diberikan informasi terkait prasyarat keamanan informasi Diskominfo Kab. Kendal dan harus menandatangani perjanjian kerahasiaan.

19.7. Kewajiban Pihak Ketiga dan tingkat layanan harus ditetapkan secara formal dalam kontrak kerja.

19.8. Metode komunikasi antara Diskominfo Kab. Kendal dan Pihak Ketiga harus ditetapkan terutama terkait penanganan insiden.

## 20. MENGATASI KEAMANAN INFORMASI DALAM PERJANJIAN DENGAN PIHAK KETIGA

20.1. Perjanjian dengan Pihak Ketiga harus mencakup klausul kerahasiaan informasi yang disetujui oleh Pihak Ketiga.

20.2. Setiap personel Pihak Ketiga yang dapat mengakses, memproses, menyimpan, berkomunikasi, atau mengkonfigurasi komponen infrastruktur TIK, dan informasi untuk organisasi harus menandatangani perjanjian kerahasiaan informasi.

## 21. SUPPLY CHAIN DARI TEKNOLOGI INFORMASI DAN KOMUNIKASI

21.1. *Supply Chain* dari teknologi informasi dan komunikasi harus mencakup kebutuhan untuk mengatasi risiko terkait dengan keamanan informasi dan layanan teknologi dan produk *supply chain*.

21.2. Jika penyediaan layanan yang diberikan Pihak Ketiga melibatkan subkontraktor, maka Pihak Ketiga harus memastikan prasyarat keamanan informasi yang diberikan Diskominfo Kab. Kendal akan dipenuhi juga oleh subkontraktornya.

21.3. Pihak Ketiga harus melaksanakan proses pemantauan untuk memastikan bahwa pengiriman produk dan jasa yang diberikan subkontraktor mengikuti persyaratan keamanan informasi yang diberikan Diskominfo Kab. Kendal.

## 22. PEMANTAUAN, PENINJAUAN DAN PENGELOLAAN PERUBAHAN LAYANAN DARI PIHAK KETIGA

22.1. Pemantauan terhadap layanan yang disediakan oleh Pihak Ketiga meliputi antara lain:

22.1.1. Memantau tingkat layanan yang diberikan sesuai dengan perjanjian kerja.

22.1.2. Mengkaji laporan yang disampaikan oleh Pihak Ketiga dengan melakukan pertemuan berkala yang dituangkan dalam risalah rapat atau laporan progress pelaksanaan pekerjaan Pihak Ketiga.

22.2. Layanan, laporan dan *record* yang diberikan oleh Pihak Ketiga harus secara rutin diawasi dan ditinjau. Selain itu audit terhadap layanan, laporan dan *record* tersebut perlu dilakukan secara rutin.

22.3. Pengawasan dan peninjauan kinerja Pihak Ketiga harus memastikan bahwa persyaratan dan ketentuan yang terkait dengan keamanan informasi dalam perjanjian kerja telah dijalankan dengan baik, dan insiden maupun masalah keamanan informasi telah dikelola dengan tepat.

22.4. Proses ini mencakup hubungan dan proses pengelolaan layanan antara organisasi dan Pihak Ketiga untuk melaksanakan:

22.4.1. Memberikan informasi terkait dengan insiden keamanan informasi dan meninjau laporan terkait dengan insiden keamanan informasi yang diberikan oleh Pihak Ketiga.

22.4.2. Meninjau *audit trail*, *security event*, permasalahan operasional, dan kegagalan dari Pihak Ketiga.

22.4.3. Menyelesaikan dan mengelola permasalahan yang telah teridentifikasi.

22.5. Bila diperlukan, dapat dilakukan audit terhadap Pihak Ketiga untuk memastikan kinerja dan pelayanan yang diberikan telah sesuai dengan perjanjian atau kontrak yang telah ditetapkan.

22.6. Seluruh perubahan terhadap layanan yang diberikan oleh Pihak Ketiga, termasuk operasional dan pemeliharaan harus dikelola dengan mempertimbangkan sistem yang dijalankan oleh Diskominfo Kab. Kendal

22.7. Manajemen perubahan untuk layanan Pihak Ketiga harus mempertimbangkan hal-hal berikut:

22.7.1. Perubahan yang diterapkan organisasi untuk mengimplementasikan:

- Peningkatan layanan organisasi.
- Pengembangan sistem dan aplikasi informasi baru.
- Modifikasi atau update kebijakan dan prosedur yang dimiliki organisasi
- Kontrol baru untuk mengatasi insiden keamanan informasi dan untuk meningkatkan keamanan informasi organisasi.

22.7.2. Perubahan dalam layanan Pihak Ketiga untuk mengimplementasikan:

- Perubahan dan peningkatan jaringan komunikasi.
- Penggunaan teknologi baru.
- Penggunaan produk baru atau versi terbaru.
- *Tools* dan lingkungan pengembangan baru.
- Perubahan lokasi pengerjaan.
- Perubahan vendor.

## 23. KEAMANAN INFORMASI DALAM PENGGUNAAN LAYANAN CLOUD

23.1. Penggunaan layanan *cloud* perlu mencakup proses evaluasi dan seleksi penyedia layanan *cloud* yang memenuhi standar keamanan informasi.

23.2. Penyedia layanan *cloud* memiliki prosedur pengelolaan identitas dan akses pengguna terhadap lingkungan *cloud* seperti penggunaan autentikasi yang kuat, manajemen kunci enkripsi, serta pemantauan aktivitas pengguna untuk mendeteksi ancaman atau perilaku yang mencurigakan.

23.3. Penyedia layanan *cloud* memiliki protokol komunikasi yang aman saat data bergerak antara organisasi dan penyedia layanan *cloud*, serta penggunaan enkripsi data yang kuat saat data disimpan di *cloud*

23.4. Penyedia layanan *cloud* memiliki rencana pemulihan insiden dan keberlanjutan bisnis yang relevan dengan lingkungan *cloud* yang mencakup kesiapan infrastruktur, pengujian pemulihan bencana, dan analisis dampak bisnis

23.5. Tanggung jawab penyedia layanan *cloud* dalam memastikan kepatuhan dalam memenuhi regulasi atau standar keamanan yang berlaku.

## 24. PERENCANAAN DAN PERSIAPAN PENANGANAN INSIDEN KEAMANAN INFORMASI

24.1. Diskominfo Kab. Kendal mempunyai tanggung jawab untuk memastikan penanganan insiden informasi pada data center yang mempunyai kewenangan dalam mengoordinasikan tindak lanjut insiden telah dijalankan dengan cepat dan efektif.

24.2. Selain pelaporan kejadian dan kelemahan keamanan informasi, proses pengawasan (*monitoring*) dari sistem, *alerts* dan kerentanan (*vulnerability*) juga perlu digunakan untuk mendeteksi insiden keamanan informasi. Beberapa aspek berikut perlu dipertimbangkan dalam prosedur insiden keamanan informasi organisasi.

24.2.1. Prosedur perlu dibuat untuk menangani berbagi tipe insiden keamanan informasi, yang meliputi namun tidak terbatas pada:

- *Malware—virus, worm, trojan horse,* atau jenis program jahat lainnya yang berhasil menginfeksi suatu *host*.
- *Denial of service*—suatu serangan yang mengakibatkan penolakan atau gangguan atas penggunaan sistem, jaringan, atau aplikasi.
- *Multiple Component* suatu insiden yang merupakan gabungan dari beberapa jenis insiden.
- Kesalahan (*error*) yang diakibatkan oleh data bisnis yang tidak lengkap atau tidak akurat.
- Kebocoran informasi yang menyebabkan hilangnya aspek kerahasiaan dan integritas informasi.
- Penyalahgunaan sistem informasi.
- Ketidakpatuhan terhadap kebijakan dan prosedur yang berlaku.
- Hilangnya layanan, peralatan atau fasilitas pengolahan informasi.
- Kerusakan pada perangkat lunak maupun perangkat keras.

24.2.2. Selain dari rencana penanggulangan, prosedur juga perlu mencakup:

- Analisa dan identifikasi penyebab dari insiden.
- Menjaga agar insiden yang terjadi tidak melebar (*containment*).
- Perencanaan dan implementasi tindakan korektif, bila diperlukan, untuk mencegah terulangnya insiden tersebut.
- Komunikasi dengan pihak-pihak yang terpengaruh atau terlibat dalam pemulihan dari insiden tersebut.
- Pelaporan tindakan yang dilakukan kepada pihak yang berwenang.
    - Pengumpulan bukti atau audit *trail* beserta pengamanannya untuk:
        a. Analisa permasalahan secara internal.

b. Digunakan sebagai bukti forensik untuk mencari potensi pelanggaran kontrak, regulasi atau digunakan sebagai bukti dalam proses hukum.
c. Negosiasi kompensasi dari Pihak Ketiga

- Tindakan pemulihan dari pelanggaran keamanan serta mengoreksi kegagalan sistem harus dikendalikan secara formal dan secara hati-hati untuk menjamin:
  a. Hanya pegawai yang berwenang yang mengakses data dan sistem yang berjalan (*live*).
  b. Seluruh tindakan darurat terdokumentasi dengan baik dan detail.
  c. Tindakan darurat dilaporkan kepada manajemen dan ditinjau dengan semestinya.

24.3. Personel yang memiliki tugas dan tanggung jawab pengelolaan insiden keamanan informasi harus memahami proses beserta prioritas penanganan insiden keamanan informasi.

24.4. Dalam melaksanakan penanganan insiden apabila diperlukan dapat melibatkan unit lain yang terkait.

24.5. Apabila diperlukan dan memungkinkan, koordinasi dengan Pihak Ketiga dapat dilakukan untuk mengoordinasikan tindakan serta membagi informasi mengenai insiden keamanan informasi.

## 25. ASSESSMENT DARI DAN TERHADAP KEJADIAN KEAMANAN INFORMASI

25.1. *Assessment* dari dan keputusan terhadap kejadian keamanan informasi harus diputuskan dan harus diklasifikasikan sebagai insiden keamanan informasi di mana gangguan tersebut menyebabkan hilangnya aspek kerahasiaan, integritas, dan ketersediaan informasi.

25.2. Klasifikasi prioritas insiden dapat membantu dampak dan tingkat insiden

## 26. RESPON TERHADAP INSIDEN KEAMANAN INFORMASI

26.1. Respon terhadap keamanan informasi harus ditanggapi sesuai dengan prosedur yang terdokumentasi.

26.2. Insiden keamanan informasi harus ditanggapi oleh pihak yang terkait (manajemen, personel, Pihak Ketiga).

26.3. Penanganan insiden perlu memperhatikan:

26.3.1. Pengumpulan bukti terkait dengan insiden keamanan informasi;

26.3.2. Proses eskalasi penanganan insiden;

26.3.3. Dokumentasi proses penanganan;

26.3.4. Komunikasi dengan pihak-pihak yang terkena dampak dan terkait dengan insiden.

## 27. PROSES PEMBELAJARAN DARI INSIDEN KEAMANAN INFORMASI

27.1. Setiap insiden keamanan informasi yang terjadi harus dievaluasi terkait dampak dan biaya dari insiden keamanan informasi dan digunakan sebagai bahan masukan untuk proses peninjauan dari kebijakan keamanan informasi.

27.2. Diskominfo Kab. Kendal harus memiliki mekanisme untuk menghitung dampak yang timbul dari insiden keamanan informasi.

27.3. Informasi yang diperoleh dari evaluasi insiden keamanan informasi harus digunakan untuk mengidentifikasi insiden yang berulang atau yang berdampak besar.

## 28. PENGUMPULAN BUKTI (EVIDENCE)

28.1. Bukti dari tindak lanjut penanganan insiden harus dikumpulkan, disimpan, dan ditunjukkan terkait dengan proses audit dan/atau *evidence trail* di kemudian hari.

28.2. Bukti dalam bentuk kertas (*hardcopy*) perlu disimpan dengan catatan mengenai siapa yang melaporkan bukti tersebut, serta di mana dan kapan bukti itu ditemukan. Sedangkan bukti dalam bentuk *softcopy* perlu dijamin bahwa bukti tersebut dapat selalu diakses bila dibutuhkan dan bukti tersebut disimpan.

28.3. Secara umum aturan dalam pengumpulan bukti, perlu mempertimbangkan:

28.3.1. Kualitas dan kelengkapan bukti.

28.3.2. Untuk memastikan bahwa bukti yang dikumpulkan dapat digunakan dalam proses peradilan maka sistem informasi organisasi harus sesuai dengan standard atau peraturan untuk mengumpulkan dan menghasilkan bukti, misal dengan menerapkan log sistem atau audit trail.

28.3.3. Untuk mencapai kualitas dan kelengkapan bukti, maka kualitas dan kelengkapan dari kontrol yang digunakan untuk melindungi bukti selama proses pengumpulan bukti, termasuk penyimpanan dan pengolahan bukti, perlu didukung dengan proses audit dan/atau *evidence trail* yang baik.

## 29. KEBERLANJUTAN KEAMANAN INFORMASI

29.1. Prasyarat untuk keberlanjutan keamanan informasi harus ditentukan dan diintegrasikan dengan prasyarat keberlanjutan bisnis organisasi;

29.2. Prasyarat tersebut mencakup teknik, metode atau infrastruktur yang diperlukan untuk

menjamin keberlanjutan dari keamanan informasi di Diskominfo Kab. Kendal, pada saat dan setelah terjadinya gangguan besar atau bencana;

29.3. Diskominfo Kab. Kendal harus menetapkan, mendokumentasikan, mengimplementasikan dan memelihara 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;

29.4. Diskominfo Kab. Kendal harus memverifikasi 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;

29.5. Prasyarat keamanan informasi dapat diintegrasikan pada siklus proses *business continuity management* yang mencakup :

29.5.1. Memahami kebutuhan organisasi;

29.5.2. Menentukan strategi BCM;

29.5.3. Mengembangkan dan mengimplementasikan rencana penanggulangan/ keberlanjutan bisnis;

29.5.4. Pengujian, pemeliharaan dan peninjauan rencana penanggulangan/ keberlanjutan bisnis;

29.6. Proses *business continuity management* harus dikembangkan dan dipelihara dengan mempertimbangkan kebutuhan keamanan informasi untuk keberlangsungan bisnis Diskominfo Kab. Kendal dengan mempertimbangkan :

29.6.1. Pemahaman terhadap berbagai risiko yang dihadapi Diskominfo Kab. Kendal terhadap insiden pada operasional atau keadaan darurat yang disebabkan oleh bencana alam yang mencakup prioritisasi dari proses bisnis kritikal.

29.6.2. Indentifikasi dari seluruh aset yang digunakan oleh proses bisnis kritikal.

29.6.3. Pengembangan dan dokumentasi dari *business continuity plan* yang mencakup strategi *business continuity*.

29.6.4. Pengalokasian tugas dan tanggung jawab proses *business continuity* dalam proses dan struktur Diskominfo Kab. Kendal.

29.7. Diskominfo Kab. Kendal harus menetapkan tim penanggulangan dan pemulihan bencana dan menetapkan koordinasi pemulihan BCP dalam kerangka kerja *business continuity plan*.

29.8. Proses perencanaan keberlanjutan keamanan informasi harus berfokus pada prasyarat keamanan informasi organisasi.

29.9. Rencana keberlanjutan keamanan informasi perlu mempertimbangkan kerentanan (*vulnerability*) dari organisasi termasuk dalam hal tersebut adalah informasi sensitif

yang dimiliki. Hal ini diperlukan untuk merencanakan tindakan untuk memastikan kerentanan tersebut dapat dikendalikan dan dikelola dengan baik.

29.10. Setiap proses atau rencana dalam rencana keberlanjutan keamanan informasi, seperti prosedur darurat atau rencana manual untuk *fallback*, perlu memiliki pemilik proses (*process owner*) yang khusus dan akan bertanggung jawab untuk mengelola proses atau rencana tersebut. Hal ini termasuk proses atau rencana yang melibatkan Pihak Ketiga penyedia jasa.

29.11. Diskominfo Kab. Kendal 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.

29.12. Penanggung jawab sistem di Diskominfo Kab. Kendal 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.

29.13. Proses perencanaan dan pengembangan *business continuity plan* meliputi :

29.13.1. Identifikasi dan kesepakatan untuk semua tanggung jawab pada tim BCP di Diskominfo Kab. Kendal yang terlibat dalam pemulihan proses darurat.

29.13.2. Melengkapi prosedur operasional bisnis pada proses *recovery* dan *restoration*.

29.13.3. Rencana pelatihan untuk personel yang terlibat dalam proses-proses dalam *business continuity plan*.

29.13.4. Pengujian dari *business continuity plan*.

29.14. Diskominfo Kab. Kendal harus memastikan dokumen BCP yang disimpan dan selalu *up-to-date*.

29.15. 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.

29.16. Sebuah rencana atau skenario pengujian perlu disusun dan berisi bagaimana dan dalam frekuensi apa setiap elemen rencana keberlanjutan keamanan informasi akan diuji.

29.17. Beberapa cara berikut perlu digunakan untuk menjamin rencana keberlanjutan keamanan informasi dapat berjalan dalam kondisi nyata.

29.17.1. Pengujian melalui simulasi di atas kertas (*table-top testing*) dari 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.

29.17.2. 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.

29.17.3. Pengujian pemulihan sistem secara teknis untuk memastikan bahwa sistem informasi organisasi dapat di-restore dengan baik.

29.17.4. Pengujian pemulihan (*recovery*) menggunakan fasilitas pada lokasi alternatif. Hal ini dilakukan dengan menjalankan proses bisnis pada lokasi utama secara paralel dengan proses bisnis pada fasilitas *recovery* pada lokasi alternatif.

29.17.5. Pengujian fasilitas dan layanan yang disediakan oleh Pihak Ketiga untuk menjamin layanan yang disediakan oleh supplier eksternal sesuai dengan perjanjian dalam kontrak kerja.

29.17.6. Pengujian secara menyeluruh dengan melibatkan seluruh komponen organisasi termasuk pegawai, peralatan, fasilitas serta proses bisnis organisasi untuk menjamin kesiapan seluruh komponen organisasi dalam menghadapi gangguan bisnis.

29.17.7. Hasil pengujian rencana keberlanjutan keamanan informasi perlu didokumentasi secara komprehensif untuk kemudian ditinjau untuk mencari tindakan-tindakan perbaikan yang dapat diambil untuk menyempurnakan rencana keberlanjutan keamanan informasi tersebut.

29.18. Peninjauan secara berkala terhadap rencana keberlanjutan keamanan informasi perlu dilakukan untuk menjamin rencana yang ada tetap sesuai dengan perubahan dan/atau perkembangan bisnis organisasi. Perubahan yang terjadi terhadap rencana keberlanjutan keamanan informasi perlu dilakukan secara formal dan kemudian didistribusikan kepada seluruh komponen dalam organisasi.

29.19. Contoh dari perubahan dan/atau perkembangan bisnis yang dapat menjadi bahan pertimbangan perubahan rencana keberlanjutan keamanan informasi adalah pembelian perangkat baru, *upgrade* sistem serta perubahan pada :

29.19.1. Personel

29.19.2. Alamat, lokasi, fasilitas dan sumber daya kerja

29.19.3. Kontrol keamanan informasi.

## 30. KESIAPAN TIK DALAM KEBERLANGSUNGAN BISNIS

30.1. Diskominfo Kab. Kendal memastikan bahwa sistem teknologi informasi dan komunikasi (TIK) siap menghadapi dan bertahan dari gangguan atau insiden yang dapat mengganggu operasional bisnis.

30.2. Tujuan untuk mempersiapkan TIK untuk meminimalkan dampak yang timbul terhadap kontinuitas bisnis dan memastikan dukungan TIK dalam kelangsungan operasional yang optimal.

30.3. Diskominfo Kab. Kendal melakukan identifikasi dan penilaian terhadap aset TIK yang paling kritis bagi kelangsungan bisnis. Aset kritis termasuk sistem, aplikasi, data, dan infrastruktur yang diperlukan serta penetapan prioritas pemulihan dan alokasi sumber daya.

30.4. Keterlibatan TIK dalam keberlangsungan bisnis mengikuti proses keberlangsungan bisnis.

## 31. IDENTIFIKASI ATURAN HUKUM, REGULASI MAUPUN KONTRAK YANG BERLAKU

31.1. Diskominfo Kab. Kendal harus mengidentifikasi semua persyaratan legal, regulasi, dan kontraktual secara terdokumentasikan untuk memastikan kesesuaiannya dengan peraturan/perundang-undangan yang berlaku secara nasional terhadap proses keamanan informasi yang diijalankan.

31.2. Diskominfo Kab. Kendal harus mendokumentasikan metode dan kontrol yang digunakan untuk memastikan kepatuhan terhadap prasyarat tersebut. Alokasi tugas dan tanggung jawab untuk memastikan kepatuhan juga harus dilakukan.

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

## 32. HAK ATAS KEKAYAAN INTELEKTUAL (HAKI)

32.1. Diskominfo Kab. Kendal harus memastikan penggunaan aset TI yang memiliki HAKI dan produk *software* berlisensi telah memenuhi kepatuhan terhadap peraturan, dan kebutuhan kontrak.

32.2. Terkait dengan pengelolaan *software* di Diskominfo Kab. Kendal, harus dilaksanakan ketentuan sebagai berikut:

32.2.1. *Software* yang digunakan adalah *software* yang berlisensi.

32.2.2. Daftar Lisensi *software* ditatausahakan dengan baik, diperiksa status lisensi dan kesesuaiannya secara berkala.

32.2.3. Mencari sumber yang terpercaya untuk mendapatkan materi berlisensi untuk

menjamin tidak ada *copyright* yang dilanggar.

32.2.4. Memberikan pemberitahuan secara reguler terhadap seluruh pegawai mengenai kewajiban untuk mematuhi undang-undang terkait hak atas kekayaan intelektual termasuk pemberitahuan mengenai sanksi yang akan diberikan bagi pegawai yang melanggar kebijakan tersebut.

32.2.5. Mengelola daftar aset (*asset register*) dengan baik serta mengidentifikasi aset yang memiliki kaitan dengan kebijakan perlindungan hak atas kekayaan intelektual

32.2.6. Menyimpan bukti kepemilikan terhadap lisensi, master copy serta manual perangkat lunak maupun informasi yang terkait dengan hak atas kekayaan intelektual.

32.2.7. Mengimplementasikan pengendalian untuk menjamin jumlah lisensi yang terpasang tidak melebihi jumlah lisensi yang dimiliki.

32.2.8. Melakukan pemeriksaan secara berkala dengan perangkat audit yang sesuai untuk menjamin hanya *software* yang diizinkan dan berlisensi saja yang terpasang.

32.2.9. Mematuhi seluruh syarat dan prasyarat dari lisensi *software* atau informasi yang dimiliki.

32.2.10. Tidak melakukan proses duplikasi atau perubahan format dari *software* atau informasi dan data lainnya sesuai dengan hukum hak atas kekayaan intelektual.

## 33. PERLINDUNGAN TERHADAP RECORD

33.1. *Record* perlu dikategorikan sesuai dengan tipenya seperti *record database*, log dari transaksi atau hasil audit yang perlu dilengkapi dengan keterangan mengenai masa simpan dan masa retensi.

33.2. Catatan (*records*) yang penting bagi organisasi harus diamankan dari risiko kehilangan, kerusakan, dan pemalsuan untuk menyesuaikan undang-undang, peraturan, kontrak, dan kebutuhan bisnis.

33.3. Perhatian juga perlu diberikan mengenai kemungkinan rusaknya media penyimpanan *record* organisasi. Penyimpanan dan penanganan *record* harus disesuaikan dengan spesifikasi media penyimpanan tersebut.

33.4. Dalam memenuhi kebutuhan dan tujuan organisasi dalam melindungi *record* organisasi, beberapa langkah berikut perlu diambil :

33.4.1. Mengeluarkan aturan dan prosedur mengenai masa retensi, penyimpanan, penanganan dan pemusnahan *record* organisasi.

33.4.2. Penetapan masa retensi untuk setiap *record* organisasi.

33.4.3. Inventarisasi dari informasi yang perlu dikelola beserta sumber dari informasi tersebut.

33.4.4. Implementasi dari kontrol untuk melindungi *record* dari kerusakan, pemalsuan dan kehilangan.

## 34. PERLINDUNGAN DATA DAN INFORMASI PRIBADI

34.1. Pengamanan data dan informasi pribadi harus dipastikan telah sesuai dengan undang-undang, peraturan, dan kontrak yang berlaku.

34.2. Diskominfo Kab. Kendal harus mengembangkan dan mengimplementasikan sebuah kebijakan perlindungan data dan informasi pribadi. Kebijakan tersebut harus dikomunikasikan kepada seluruh pegawai terutama bagi pegawai yang terlibat dalam pengolahan informasi pribadi.

34.3. Sebuah struktur organisasi beserta sistem kontrolnya perlu dibuat untuk memastikan kepatuhan (*compliance*) kepada seluruh kebijakan, aturan dan regulasi yang berhubungan dengan perlindungan data. Hal ini dapat dilakukan dengan menetapkan seorang pegawai yang bertanggung jawab untuk memberikan arahan kepada pegawai lainnya mengenai tanggung jawab individu beserta prosedur yang harus diikuti terkait dengan perlindungan data dan informasi pribadi.

34.4. Dalam implementasinya, perlindungan data dan informasi pribadi perlu mempertimbangkan aspek teknologi informasi dan struktur organisasi.

34.5. Perlindungan data dan informasi pribadi perlu mempertimbangkan undang-undang dan regulasi negara yang berlaku. Perhatian lebih perlu diberikan terutama apabila dilakukannya transfer data dan informasi pribadi antarnegara.

## 35. PENINJAUAN (REVIEW) INDEPENDEN UNTUK KEAMANAN INFORMASI

35.1. Sistem keamanan informasi yang berjalan di organisasi perlu secara berkala atau pada saat terjadi perubahan besar pada sistem keamanan informasi, ditinjau (di-review) secara independen.

35.2. Tinjauan ini perlu dilakukan untuk menjamin kesesuaian, kecukupan dan efektivitas dari sistem keamanan informasi organisasi. Tinjauan ini perlu juga melihat peluang untuk perbaikan atau kebutuhan untuk perubahan pada sistem keamanan informasi, termasuk kebijakan, prosedur maupun penerapan kontrol keamanan informasi.

35.3. Tinjauan ini harus dilakukan oleh pihak yang independen dari area yang ditinjaunya, seperti tim audit internal, personel dari bagian lain yang tidak terlibat pada area yang akan ditinjau atau oleh Pihak Ketiga yang memiliki spesialisasi untuk melakukan

tinjauan keamanan informasi.

35.4. Pihak yang melakukan tinjauan harus memiliki keahlian dan pengalaman dalam bidang keamanan informasi.

35.5. Hasil dari tinjauan manajemen ini harus dilaporkan kepada pihak manajemen serta didokumentasikan. Tindakan lanjutan dapat diambil apabila terjadi ketidaksesuaian pada implementasi atau berjalannya sistem keamanan informasi.

## 36. KEPATUHAN TERHADAP KEBIJAKAN DAN STANDAR KEAMANAN INFORMASI

36.1. Pimpinan di masing-masing unit kerja harus memastikan semua prosedur keamanan dalam area kerjanya telah dijalankan dengan benar dan telah sesuai dengan kebijakan dan standar keamanan informasi organisasi.

36.2. Diskominfo Kab. Kendal harus secara reguler melakukan tinjauan terhadap kepatuhan dari sistem informasi, termasuk penggunaan fasilitas pengolahan informasi, proses penanganan informasi dalam lingkup bagiannya sesuai dengan kebijakan, standar dan *requirement* keamanan informasi yang berlaku.

36.3. Apabila tinjauan tersebut menemukan adanya ketidakpatuhan (*non-compliance*), maka manajer tersebut harus:

36.3.1. Menentukan penyebab dari ketidakpatuhan.

36.3.2. Menentukan perlunya tindakan untuk mencegah terulangnya ketidakpatuhan.

36.3.3. Menentukan dan mengimplementasikan tindakan korektif yang sesuai.

36.3.4. Meninjau tindakan korektif yang telah diambil.

36.4. Hasil dari tinjauan dan tindakan korektif yang diambil harus didokumentasikan serta *records* yang dihasilkan harus selalu dipelihara.

36.5. Hasil tinjauan harus dilaporkan kepada pihak yang berkepentingan sebagai bahan untuk tindakan lanjutan.

36.6. Penanggung jawab sistem di Diskominfo Kab. Kendal harus memeriksa sistem secara berkala untuk memastikan kesesuaian terhadap standar penerapan keamanan yang ditetapkan melalui pemeriksaan secara teknis dari sisi perangkat lunak maupun perangkat keras sesuai dengan spesifikasi yang telah ditetapkan.

36.7. Apabila pemeriksaan *technical compliance* mencakup pelaksanaan *penetration testing* atau *vulnerability assessment*, maka kegiatan test tersebut perlu direncanakan dan didokumentasikan dengan baik untuk mencegah risiko gangguan terhadap keamanan dari sistem informasi serta untuk memastikan bahwa kegiatan test tersebut memenuhi aspek *repeatable*.

36.8. Pemeriksaan tersebut dapat dilakukan secara manual maupun otomatis untuk

kemudian menghasilkan laporan teknis yang dapat dianalisa oleh personel yang kompeten.

36.9. Setiap pemeriksaan *technical compliance* harus dilakukan oleh atau dilakukan di bawah pengawasan personel yang kompeten dan berwenang.

## 37. PROSEDUR OPERASIONAL YANG TERDOKUMENTASI

37.1. Setiap sistem yang dioperasikan di lingkungan Diskominfo Kab. Kendal harus dilengkapi dengan prosedur dan petunjuk pengoperasian (misalnya *Run Book* atau *Manual Book*) dan dipelihara untuk menjaga ketersediaan bagi seluruh pengguna sistem informasi yang membutuhkannya.

37.2. Prosedur operasional perlu secara spesifik memberikan detail mengenai pelaksanaan kegiatan yang mencakup:

37.2.1. Pengelolaan kapasitas.

37.2.2. Pengelolaan perubahan.

37.2.3. *Backup* dan *restore*.

37.2.4. Prosedur penanganan insiden/gangguan selama aktivitas pekerjaan berlangsung.

37.2.5. Pihak yang harus dihubungi untuk mendapatkan dukungan (*support*) apabila terjadi masalah atau kesulitan.

37.2.6. Proses *restart* dan *recovery* sistem.

37.3. Seluruh dokumentasi dari prosedur operasional harus ditangani sesuai klasifikasinya dan sesuai dengan proses pengelolaan dokumentasi organisasi.

# BAB III KENDALI KEAMANAN INFORMASI ASPEK SUMBER DAYA MANUSIA

## 1. PENYARINGAN (*SCREENING*)

1.1. Sebelum bekerja dilakukan pemeriksaan (*screening*) dan verifikasi latar belakang calon pegawai Diskominfo Kab. Kendal dan Pihak Eksternal.

1.2. Penerimaan pegawai di lingkungan Diskominfo Kab. Kendal harus sesuai dengan ketentuan yang berlaku.

## 2. SYARAT DAN KETENTUAN PEGAWAI

2.1. Setiap pegawai dan Pihak Eksternal pada Diskominfo Kab. Kendal bertanggung jawab untuk menjaga keamanan informasi Diskominfo Kab. Kendal

2.2. Setiap pengguna informasi maupun sistem informasi organisasi harus menyetujui dan menandatangani syarat dan ketentuan terkait dengan keamanan informasi dan sistem informasi organisasi.

2.3. Untuk menjaga keamanan informasi dan kepatuhan tenaga kontrak wajib membuat dan menandatangani NDA (*Non-Disclosure Agreement*).

## 3. MEMBANGUN KESADARAN TERKAIT KEAMANAN INFORMASI

3.1. Sosialisasi dan pelatihan mengenai keamanan informasi kepada semua Pegawai Diskominfo Kab. Kendal dan Pihak Ketiga harus dilakukan secara berkala sesuai dengan tugas dan wewenang yang diberikan.

## 4. PROSES PENDISIPLINAN

4.1. Setiap pegawai Diskominfo Kab. Kendal yang melakukan pelanggaran terkait keamanan informasi harus dilakukan proses pendisiplinan secara formal sesuai dengan tata tertib organisasi.

4.2. Kepala Diskominfo Kab. Kendal harus mempertimbangkan bentuk sanksi yang tegas sesuai dengan tingkat pelanggaran yang dilakukan.

## 5. PEMBERHENTIAN ATAU PERGANTIAN STATUS PEGAWAI

Proses ini dilakukan untuk menjamin proses pemberhentian atau pergantian tugas dan fungsi pengguna informasi atau sistem informasi berjalan dengan baik. Tanggung jawab pengelolaan proses ini perlu diberikan kepada pegawai atau unit kerja tertentu untuk

menjamin pengembalian informasi, Aset informasi, dan hak akses telah dilakukan. Proses ini perlu dilakukan secara transparan untuk menjamin tidak adanya kebocoran informasi karena ketidaktahuan dari pengguna atau rekan pengguna akan adanya proses pemberhentian atau pergantian status kepegawaian. Beberapa hal yang perlu diperhatikan saat terjadi pemberhentian atau pergantian status pegawai adalah sebagai berikut:

5.1. Dalam hal terjadi proses perubahan atau terminasi hubungan kerja maka dilakukan langkah-langkah untuk melindungi kepentingan Diskominfo Kab. Kendal dengan mendefinisikan, mengomunikasikan dan memberlakukan tanggung jawab dan tugas Keamanan Informasi kepada pegawai dan Pihak Eksternal.

5.2. Tanggung jawab pegawai pada saat dan setelah proses pemberhentian atau pergantian status kepegawaian harus dikomunikasikan dengan jelas kepada personel yang bersangkutan.

## 6. PERJANJIAN KERAHASIAAN

6.1. Setiap pegawai Diskominfo Kab. Kendal 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 Diskominfo Kab. Kendal

6.2. Perjanjian Kerahasiaan perlu dibuat dan disetujui secara formal melalui proses penandatanganan oleh seluruh pihak baik internal maupun eksternal yang mengakses informasi maupun sistem informasi Diskominfo Kab. Kendal yang tidak bersifat publik.

6.3. Perjanjian Kerahasiaan akan secara hukum mendukung perlindungan informasi dan sistem informasi Diskominfo Kab. Kendal dari risiko pengungkapan (*disclosure*) tanpa izin.

6.4. Dalam penyusunan perjanjian kerahasiaan beberapa aspek berikut perlu dipertimbangkan:

6.4.1. Pendefinisian dan identifikasi dari informasi yang perlu dilindungi.

6.4.2. Durasi / masa berlakunya perjanjian kerahasiaan, hal ini perlu mempertimbangkan sensitivitas dan masa retensi dari informasi dan sistem informasi yang terkait.

6.4.3. Tanggung jawab dan tindakan yang harus diambil pihak yang menandatangani perjanjian untuk menghindari pengungkapan (*disclosure*) informasi tanpa izin.

6.4.4. Kepemilikan dari informasi, rahasia dan kekayaan intelektual, berhubungan dengan perlindungan dari kerahasiaan informasi tersebut.

6.4.5. Panduan mengenai bagaimana informasi rahasia boleh digunakan.

6.4.6. Hak untuk melakukan audit dan memantau aktivitas penanda tangan perjanjian.

6.4.7. Proses pemberitahuan dan pelaporan apabila terjadi pengungkapan tanpa izin atau kebocoran informasi.

6.4.8. Tindakan yang akan dilakukan apabila terjadi pelanggaran perjanjian.

6.4.9. Perjanjian harus selaras dengan peraturan perundang-undangan dan regulasi yang berlaku.

## 7. REMOTE WORKING

7.1. Aktivitas *remote working* yang dilakukan di luar lingkungan Diskominfo Kab. Kendal harus dipastikan bahwa area yang digunakan sudah aman dari akses oleh pihak yang tidak terotorisasi baik disengaja maupun tidak disengaja.

7.2. Pegawai yang dapat melakukan *remote working* harus mendapatkan otoritas dari Koordinator dan Pimpinan terkait.

## 8. PELAPORAN KEJADIAN DALAM KEAMANAN INFORMASI

8.1. Seluruh pegawai Diskominfo Kab. Kendal harus melaporkan insiden keamanan informasi yang teridentifikasi secepat mungkin melalui mekanisme pelaporan insiden di Diskominfo Kab. Kendal

8.2. Prosedur formal pelaporan kejadian dalam sistem keamanan informasi perlu dibuat bersama dengan prosedur penanganan dan eskalasinya yang menjabarkan tindakan yang harus diambil pada saat penerimaan laporan.

8.3. Sebuah *point of contact* perlu dibuat untuk menerima laporan tersebut. Perlu dipastikan juga bahwa *point of contact* ini diketahui oleh pengguna sistem informasi organisasi, selalu tersedia dan dapat memberikan tanggapan secara tepat dan cepat untuk setiap laporan.

8.4. Seluruh pengguna sistem informasi, baik pegawai, kontraktor atau Pihak Ketiga harus memahami tanggung jawabnya untuk secepat mungkin melaporkan kejadian keamanan informasi. Mereka juga harus memahami prosedur pelaporan kejadian dalam sistem informasi organisasi beserta *point of contact* untuk melaporkan kejadian tersebut. Prosedur pelaporan itu perlu mencakup antara lain:

8.4.1. Sebuah proses *feedback* yang memastikan pemberitahuan kepada pelapor, setelah laporannya telah selesai ditindaklanjuti.

8.4.2. 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 kejadian keamanan informasi.

8.4.3. Tindakan yang harus diambil apabila terjadi kejadian dalam sistem keamanan informasi seperti:

- Mencatat dengan segera seluruh detail kejadian seperti tipe dari kejadian atau *non-compliance*, kerusakan yang terjadi atau pesan kesalahan pada sistem.
- Tidak mengambil tindakan sendiri, melainkan segera melaporkan kepada *point of contact* yang telah ditetapkan.

8.4.4. Referensi ke proses disiplin formal yang telah ditetapkan untuk menangani pegawai, Pihak Ketiga yang melakukan pelanggaran keamanan informasi.

- Contoh dari kejadian mencakup namun tidak terbatas pada daftar berikut:
  - Tidak efektifnya kontrol keamanan informasi.
  - Kegagalan atau *overload* dari sistem informasi.
  - Kesalahan manusia.
  - *Non-compliance* dengan kebijakan dan prosedur.
  - Tembusnya pengamanan fisik dan lingkungan.
  - Pergantian sistem yang tidak terkendali.
  - Kegagalan fungsi perangkat lunak dan keras.
  - Pelanggaran hak akses.
- Semua pegawai Diskominfo Kab. Kendal yang menggunakan sistem wajib melaporkan kelemahan dalam sistem dan jaringan secepat mungkin untuk mencegah terjadinya insiden keamanan informasi.
- Seluruh pengguna sistem informasi organisasi, termasuk pegawai dan Pihak Ketiga, harus melaporkan kelemahan dalam sistem keamanan informasi organisasi secepat mungkin melalui mekanisme yang telah disepakati sebelumnya untuk mencegah terjadinya insiden keamanan informasi. Mekanisme pelaporan tersebut harus mudah untuk diakses dan selalu tersedia.
- Pelapor harus diinformasikan bahwa mereka dilarang untuk membuktikan sendiri dugaan kelemahan yang ditemukan, seperti dengan melakukan *penetration testing* tanpa izin.

# BAB IV KENDALI KEAMANAN INFORMASI ASPEK FISIK DAN LINGKUNGAN

## 1. PERIMETER KEAMANAN FISIK

1.1. Pembatasan wilayah dengan pembatas secara fisik harus digunakan untuk melindungi area yang berisi informasi dan/atau fasilitas pengolahan informasi.

1.2. Pengamanan fisik ruangan di lingkungan Diskominfo Kab. Kendal mengacu kepada klasifikasi wilayah masing-masing ruangan dengan menggunakan pembatas dan pengendalian akses fisik (berupa: kartu kontrol akses, fingerprint, PIN).

1.3. Akses ke dalam area organisasi harus dibatasi dengan antara lain 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.

1.4. Akses ke dalam area organisasi harus dipantau untuk mendeteksi aktivitas yang dapat menimbulkan kerugian organisasi.

1.5. Fasilitas pemrosesan informasi harus diletakkan di dalam ruangan yang memiliki kontrol pengamanan akses keluar masuk yang memadai.

1.6. Fasilitas pemrosesan informasi organisasi harus terpisah secara fisik dari area kerja Pihak Ketiga.

1.7. Pintu darurat perlu dilengkapi dengan alarm yang dimonitor dan diuji secara berkala untuk memastikan berfungsi sebagaimana mestinya.

## 2. PENGENDALIAN AKSES FISIK AREA KEAMANAN KHUSUS

2.1. Akses fisik area keamanan khusus harus dikendalikan untuk menjamin tidak adanya akses tanpa izin.

2.2. Tamu atau Pihak Ketiga yang datang ke area keamanan khusus di lingkungan Diskominfo Kab. Kendal dicatat tanggal dan waktu masuk maupun keluarnya, harus tetap didampingi atau diawasi kecuali telah mendapatkan izin akses. Pengunjung perlu diberi informasi mengenai syarat keamanan area keamanan khusus beserta prosedur dalam keadaan darurat.

2.3. Tamu atau Pihak Ketiga yang mengakses area kritikal di Diskominfo Kab. Kendal hanya untuk pegawai yang mempunyai kewenangannya dan diotorisasi oleh Pejabat penanggung jawab di ruang tersebut dan harus diawasi dan didampingi oleh pegawai di ruangan tersebut.

2.4. Akses masuk ke dalam area tempat pemrosesan/penyimpanan informasi sensitif harus dikendalikan menggunakan *dual authentication* seperti kombinasi fingerprint, kartu akses atau PIN. *Audit trail* terkait akses ke dalam area tersebut harus dikelola dengan baik.

2.5. Semua pengguna baik internal maupun eksternal wajib mengenakan ID Card ketika masuk ke dalam area keamanan khusus. Pengguna harus segera melaporkan kepada petugas yang berwenang seandainya ditemukan pengguna yang tidak mengenakan ID Card.

2.6. Hak akses ke area keamanan khusus harus selalu ditinjau secara rutin.

2.7. Akses di wilayah loading area yang dapat memasuki area keamanan khusus di Diskominfo Kab. Kendal harus diamankan untuk menghindari akses tanpa izin.

2.8. Dalam mengamankan area tersebut beberapa hal tersebut perlu dilakukan:

2.8.1. Akses ke area tersebut harus dibatasi untuk personel yang telah terdaftar dan terotorisasi.

2.8.2. *Delivery* dan *loading area* harus ditempatkan di mana personel yang mengakses area tersebut tidak perlu memasuki area terbatas dan tertutup organisasi.

2.8.3. Pintu masuk ke *delivery* dan *loading area* harus diamankan.

2.8.4. Barang-barang yang datang dari luar harus didaftarkan dan diperiksa sebelum dipindahkan ke area internal organisasi.

## 3. PENGAMANAN RUANG KANTOR DAN FASILITASNYA

3.1. Ruangan kerja dan fasilitas di lingkungan Diskominfo Kab. Kendal perlu diberikan pengamanan secara memadai dengan mempertimbangkan pemisahan dari wilayah akses umum.

3.2. Untuk area kritikal dan/atau area keamanan khusus di Diskominfo Kab. Kendal tidak dipasang informasi/petunjuk lokasi yang jelas.

3.3. Apabila memungkinkan, fasilitas yang digunakan untuk pemrosesan dan penyimpanan informasi sensitif sebaiknya terpisah dengan fasilitas yang digunakan untuk pekerjaan sehari-hari.

3.4. Dalam mengamankan ruangan tersebut beberapa hal berikut perlu dipertimbangkan :

3.4.1. Perhatian perlu diberikan terhadap aspek kesehatan dan keamanan berdasarkan standar maupun regulasi yang terkait.

3.4.2. Kantor, ruang kerja dan fasilitas organisasi perlu didesain sedemikian rupa untuk meminimalisasi akses oleh masyarakat umum.

## 4. PEMANTAUAN KEAMANAN FISIK

4.1. Pengendalian akses fisik ke fasilitas atau area yang mengandung aset informasi sensitif mencakup penggunaan kartu akses, penggunaan sistem penguncian serta pengawasan terhadap tamu atau pengunjung yang masuk ke area terbatas.

4.2. Pengawasan keamanan area fisik dapat menggunakan kamera pengawas (CCTV), sistem deteksi kebakaran, pengawasan petugas keamanan, dan pemantauan lalu lintas orang dan barang yang masuk dan keluar dari area tersebut.

4.3. Pemeliharaan rutin dan pengujian peralatan keamanan fisik, seperti sistem alarm, kamera pengawas, atau sistem penguncian untuk memastikan bahwa peralatan berfungsi dengan baik dan dapat memberikan perlindungan yang diperlukan.

## 5. PERLINDUNGAN TERHADAP ANCAMAN EKSTERNAL DAN LINGKUNGAN

5.1. Peralatan pemadam kebakaran yang memadai harus tersedia pada tempat yang sesuai.

5.2. Khusus ruangan kritikal dan/atau area keamanan khusus di Diskominfo Kab. Kendal menggunakan peralatan pemadam kebakaran yang bersifat non-liquid.

5.3. Perlindungan perlu diberikan kepada area organisasi dari risiko yang muncul dari kebakaran, banjir, gempa bumi, ledakan, huru-hara dan bencana lainnya, baik disebabkan oleh alam maupun manusia.

5.4. Perlindungan tersebut perlu mempertimbangkan kondisi lingkungan sekitar area organisasi.

5.5. Beberapa hal ini perlu dipertimbangkan dalam melaksanakan proses perlindungan:

5.5.1. Material yang berpotensi menimbulkan bahaya dan mudah terbakar harus disimpan di tempat yang aman dan terpisah dari ruang aktivitas kerja.

5.5.2. Media Backup harus disimpan di tempat dengan jarak yang cukup aman dari *main site* untuk menghindari kerusakan apabila terjadi bencana di *main site*.

5.5.3. Memastikan area keamanan khusus memiliki detektor api dan asap serta pipa pembuangan air.

5.5.4. Zat pemadam api dan sistem yang digunakan harus memperhatikan keamanan terhadap peralatan dan petugas pelaksana di dalam area teknologi informasi.

5.5.5. Data Center dan area yang sensitif yang berisi peralatan komputer yang kritikal dan harus terlindungi oleh deteksi api dan sistem alarm otomatis.

5.5.6. Data Center harus berada pada lokasi yang lebih tinggi dengan detektor panas, asap, dan air.

5.5.7. Deteksi api dan sistem pemadaman harus diperiksa untuk memastikan

bahwa alat tersebut sudah terpasang dengan benar, dan harus diperiksa secara rutin paling sedikit 1 (satu) kali setiap tahun.

5.5.8. Alat pemadam api darurat harus tersedia pada lokasi yang strategis dan mudah untuk dijangkau. Instruksi penggunaannya harus ditampilkan.

5.5.9. Dilarang merokok serta membawa makan dan minum dalam area keamanan khusus.

## 6. BEKERJA DI AREA AMAN

6.1. Pekerjaan yang dilakukan oleh Pihak Ketiga di area kritikal dan/atau area keamanan khusus di lingkungan Diskominfo Kab. Kendal harus selalu diawasi oleh personel penanggung jawab area tersebut untuk menghindari kegiatan yang tidak diinginkan.

6.2. Setiap pegawai dan Pihak Ketiga dilarang merokok serta membawa makanan dan minuman ke dalam wilayah tertutup.

6.3. Pihak Ketiga yang memasuki wilayah area keamanan khusus tidak diperkenankan membawa peralatan *visual recording* (kamera, handphone berkamera).

6.4. 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.

6.5. Pintu masuk dan lokasi penting pada area keamanan khusus harus dilengkapi dengan kamera CCTV. Perekam CCTV harus disimpan pada tempat aman, dan hasil rekaman CCTV harus disimpan untuk beberapa waktu tertentu.

6.6. Area keamanan khusus yang kosong harus selalu terkunci dan secara rutin dilakukan pengecekan.

## 7. CLEAR DESK DAN CLEAR SCREEN

7.1. Seluruh pegawai di lingkungan Diskominfo Kab. Kendal harus menerapkan *clear desk* dan *screen lock/clear screen* berpassword maksimum selama 10 menit untuk menlindungi informasi yang rahasia.

7.2. Semua informasi sensitif yang berbentuk hardcopy atau yang tersimpan dalam media penyimpanan dalam lemari yang terkunci.

7.3. Komputer atau terminal harus di *log-off/screen saver lock* apabila sedang tidak digunakan atau diawasi.

7.4. Memindahkan dengan segera dokumen yang mengandung informasi sensitif dari mesin printer maupun photocopy.

7.5. Pengamanan pada tempat pengiriman dan penerimaan surat dan mesin *faxcimile* yang tidak diawasi.

## 8. PERLINDUNGAN DAN PENEMPATAN PERALATAN

8.1. Perangkat pengolahan informasi yang dianggap kritikal perlu ditempatkan secara aman termasuk membatasi sudut pandang untuk mengurangi orang yang tidak berkepentingan yang dapat melihat informasi yang ditampilkan.

8.2. Peralatan kerja milik organisasi harus ditempatkan dan dilindungi untuk mengurangi risiko ancaman yang berasal dari lingkungan (api, air, debu).

8.3. Dalam melindungi peralatan kerja milik organisasi beberapa hal berikut perlu dipertimbangkan:

8.3.1. Penempatan peralatan kerja perlu dilakukan sedemikian rupa untuk mengurangi risiko adanya akses yang tidak perlu ke area kerja.

8.3.2. Fasilitas atau peralatan pengolahan informasi perlu ditempatkan sedemikian rupa sehingga mengurangi pandangan dari orang yang tidak berwenang. Hal ini termasuk membatasi sudut pandang ke peralatan tersebut.

8.3.3. Peralatan yang membutuhkan perlindungan khusus dapat diisolasi di lokasi khusus untuk mengurangi jumlah pengamanan yang diperlukan.

8.3.4. Kontrol yang memadai harus diterapkan untuk meminimalkan risiko ancaman gangguan fisik, seperti pencurian, kebakaran, ledakan gangguan dari asap, air, petir, debu, getaran, bahan kimia, gangguan terhadap pasokan listrik, jaringan komunikasi, elektromagnetik dan vandalisasi.

- Suhu dan kelembapan dalam area keamanan khusus harus dimonitor secara rutin.
- Perlindungan dari petir perlu diimplementasikan pada bangunan, jalur listrik maupun komunikasi.

## 9. PENGAMANAN PERALATAN DI LUAR WILAYAH

9.1. Penggunaan peralatan pengolahan informasi di luar wilayah Diskominfo Kab. Kendal mempertimbangkan kebutuhan penggunaan aset tersebut.

9.2. Aset TI yang bersifat portabel seperti notebook yang dibawa ke luar area kantor tidak boleh ditinggalkan di area publik tanpa pengamanan yang memadai dengan kabel pengunci (*cable lock*) serta *password*.

9.3. Pengamanan harus dilakukan pada semua aset yang terletak di luar area organisasi (*off premises*). Pengamanan ini perlu mempertimbangkan risiko yang muncul dari penggunaan peralatan dan pekerjaan di luar area organisasi.

9.4. Penggunaan peralatan pengolahan informasi di luar area organisasi harus mendapatkan izin dari pihak pengelola/pemilik peralatan.

9.5. Dalam menerapkan pengamanan, hal-hal berikut perlu dipertimbangkan:

9.5.1. Informasi dan peralatan pengolahan informasi tidak boleh ditinggal di area umum tanpa pengawasan.

9.5.2. Instruksi dari vendor pembuat peralatan pengolahan informasi mengenai penggunaan peralatan tersebut harus dipatuhi.

9.5.3. Pengendalian keamanan bagi peralatan yang digunakan untuk bekerja dari rumah perlu melalui proses penilaian risiko untuk menentukan metode kendali keamanan yang tepat.

9.5.4. Penggunaan jasa asuransi untuk melindungi organisasi dari kerugian yang mungkin muncul dari penggunaan peralatan di luar area organisasi.

## 10. MEDIA PENYIMPANAN

Pengelolaan ini diperlukan untuk mencegah pengungkapan (*disclosure*), modifikasi, *removal* atau penghancuran dari informasi yang tersimpan dalam media penyimpanan informasi sehingga harus dilindungi secara fisik.

10.1. Media yang digolongkan sebagai media penyimpanan antara lain adalah tapes, CD, DVD, external hardisk, USB flash disk, memory card.

10.2. Media penyimpanan yang digunakan di Diskominfo Kab. Kendal perlu diregister, didokumentasikan apabila ada perubahan, dan perangkat yang digunakan mempunyai fitur keamanan yang memadai.

10.3. Data yang terkandung dalam media penyimpanan yang tidak akan digunakan kembali harus dihapus secara permanen dan dipastikan tidak dapat di-recover.

10.4. Pegawai Diskominfo Kab. Kendal harus selalu melakukan *scanning virus* terhadap media pennyimpanan (flash disk, external harddisk) untuk mencegah adanya kerusakan informasi akibat *malware*.

10.5. Semua media penyimpanan harus disimpan di tempat dan lingkungan yang aman.

10.6. Media penyimpanan yang tidak boleh digunakan untuk menyimpan informasi yang bersifat rahasia secara permanen adalah CD, DVD, USB flash disk, dan memory card.

10.7. Pemilik data/informasi atau pengelola media penyimpan data/informasi bertanggung jawab terhadap pemusnahan data/informasi.

10.8. Data/informasi yang dihapus dipastikan tidak dapat digunakan lagi, dibaca kembali, atau diduplikasi ke media lain. Proses pemusnahan media dapat dilakukan dengan menggunakan mesin shredding.

10.9. Dalam hal media penyimpan elektronis akan dialihkan peruntukannya, maka data/informasi yang tersimpan dalam media tersebut yang dimaksud harus dihapus sebelum medianya dialihkan peruntukannya.

10.10. Media penyimpanan yang tidak digunakan kembali harus dimusnahkan dengan aman

menggunakan prosedur formal yang sudah ditetapkan. Hal ini perlu dilakukan untuk meminimalisasi risiko kebocoran informasi milik organisasi.

10.11. Apabila pemusnahan media dilakukan oleh Pihak Ketiga, maka kontrol yang memadai terhadap Pihak Ketiga tersebut harus diimplementasikan.

10.12. Media yang menyimpan informasi milik organisasi harus dilindungi dari akses tanpa izin, modifikasi dan penyalahgunaan selama dalam proses pemindahan atau transportasi keluar dari area organisasi.

10.13. Beberapa hal berikut harus dipertimbangkan untuk melindungi proses pemindahan media penyimpanan informasi.

10.13.1. Penggunaan media transportasi atau kurir yang terpercaya dan memiliki tingkat keandalan tinggi.

10.13.2. Pengemasan media harus dipastikan telah dilakukan dengan baik dan disesuaikan dengan jenis dan kondisi media untuk menghindari kerusakan fisik.

## 11. SARANA PENDUKUNG

11.1. Semua sarana pendukung seperti *power supply*, genset, lampu darurat, dan *air conditioner* harus tersedia untuk mendukung kegiatan operasional area keamanan khusus, dalam hal ini Data Center Diskominfo Kab. Kendal dan dipelihara serta diperiksa secara berkala untuk memastikan sarana pendukung tersebut dapat berfungsi sebagaimana mestinya.

11.2. Peralatan pengolahan informasi harus dilindungi dari kemungkinan hilangnya pasokan listrik dan gangguan lain yang disebabkan oleh gangguan pada sarana pendukung. Penyediaan penerangan darurat perlu disediakan untuk menjamin penerangan dalam kondisi hilangnya pasokan listrik.

11.3. Kondisi suplai listrik perlu dipastikan telah sesuai dengan kebutuhan dari peralatan pengolahan informasi.

11.4. Apabila memungkinkan *emergency power off switches* dapat digunakan untuk mematikan dengan segera peralatan pengolahan informasi seandainya terjadi kondisi darurat.

11.5. Ketersediaan bahan bakar pada generator listrik harus dipastikan untuk mencukupi kebutuhan pada saat diperlukan.

11.6. Bila memungkinkan penggunaan beberapa sumber pasokan listrik dapat diimplementasikan terutama untuk peralatan pengolahan informasi yang sangat sensitif untuk mengurangi kegagalan operasi pada peralatan pengolahan informasi apabila pasokan listrik yang ada putus (*single point of failure*).

11.7. Sumber Daya Listrik di-Backup oleh UPS dan Generator, dengan prosedur yang meliputi hal-hal berikut :

11.7.1. Generator harus terpasang untuk mendukung penyediaan listrik Data Center.

11.7.2. Sumber Daya Listrik harus didukung oleh UPS/*uninterrupted power supply* atau baterai cadangan, dan harus mampu untuk mendukung kapasitas untuk periode sekurang-kurangnya 15 (lima belas) menit pada saat terjadi pemadaman listrik.

11.7.3. Ruang generator dan UPS harus aman dan terkunci. Kunci harus disimpan dan hanya dapat diberikan kepada petugas yang ditunjuk.

11.7.4. Ruang generator dan UPS harus mempunyai ventilasi yang memadai dan dilengkapi dengan sistem deteksi dan perlindungan api.

11.8. Generator dan UPS harus dipelihara dan dijaga ketersediaannya secara periodik, minimal satu bulan sekali, dan dilakukan pengetesan minimal tiga bulan sekali.

11.9. Pasokan air untuk peralatan AC dan pemadam kebakaran perlu dipastikan ketersediaannya. Terkait dengan proses pemadam kebakaran, sistem peringatan (alarm) juga harus diperiksa secara rutin.

11.10. Penyediaan jalur telekomunikasi ganda dari sisi *routing*, penyedia jaringan atau teknologi jaringan perlu dipertimbangkan untuk mengurangi risiko kegagalan komunikasi apabila salah satu jalur telekomunikasi yang ada terputus (*single point of failure*).

## 12. PENGAMANAN PENGKABELAN

12.1. Kabel listrik dan jaringan komunikasi harus terlindungi dan tidak diletakkan di area publik sehingga tidak mengalami kerusakan akibat ketidaksengajaan oleh personel maupun gigitan binatang pengerat.

12.2. Penandaan kabel digunakan di Ruang Server Jaringan untuk mempermudah penanganan apabila terjadi masalah dan menghindari kesalahan dan didokumentasikan dengan baik.

12.3. Pengamanan pengkabelan perlu mempertimbangkan beberapa hal berikut :

12.3.1. Kabel listrik dan telekomunikasi yang digunakan untuk fasilitas pemrosesan informasi harus dipasang secara aman sedemikian rupa sehingga dapat terlindungi dengan baik.

12.3.2. Kabel komunikasi harus terlindungi dari kemungkinan kerusakan maupun intersepsi seperti dengan tidak diletakkan di area publik.

12.3.3. Kabel listrik harus terpasang secara terpisah dengan kabel komunikasi.

12.3.4. Untuk sistem kritikal atau sensitif perlindungan tambahan sebagai berikut

dapat dilakukan:

- Penggunaan pelindung kabel (*armoured conduit*) dan kotak atau ruangan terkunci untuk melindungi kabel terutama pada titik terminasi atau pemeriksaan.
- Penggunaan routing maupun media transmisi alternatif.
- Penggunaan kabel fiber optic.
- Penggunaan pelindung elektromagnetik.
- Pemeriksaan teknis secara fisik untuk memastikan tidak ada peralatan yang seharusnya tidak terhubung ke sistem komunikasi.
- Pengendalian akses ke ruangan kabel dan *patch panel.*

## 13. PEMELIHARAAN PERALATAN

13.1. 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.

13.2. Dalam melakukan pemeliharaan peralatan dalam sistem informasi organisasi, beberapa hal berikut perlu dipertimbangkan:

13.2.1. Melakukan pemeliharaan peralatan secara rutin sesuai spesifikasi dan rekomendasi vendor.

13.2.2. Aktivitas pemeliharaan hanya boleh dilakukan oleh personel yang memiliki kompetensi dan mendapat izin dari pihak yang mengelola perangkat.

13.2.3. Setiap indikasi kerusakan, kerusakan yang terjadi serta perbaikan yang bersifat korektif dan preventif harus didokumentasikan dengan baik.

13.2.4. Setiap pemeliharaan perlu mempertimbangkan informasi yang terdapat di dalam peralatan tersebut.

## 14. PEMUSNAHAN ATAU PENGGUNAAN KEMBALI PERALATAN SECARA AMAN

14.1. Seluruh aset TIK yang akan dimusnahkan atau digunakan kembali harus diperiksa dan dipastikan bahwa tidak ada lagi data sensitif yang tersimpan dalam perangkat sehingga tidak dimungkinkan lagi untuk mengambil informasi yang sebelumnya terkandung di perangkat tersebut.

14.2. Peralatan pengolahan informasi yang tidak akan dipergunakan lagi dan di dalamnya terdapat informasi sensitif harus dimusnahkan secara fisik, dihapus secara permanen sehingga tidak dimungkinkan lagi untuk mengambil informasi yang sebelumnya terkandung dalam peralatan tersebut.

14.3. Peralatan pengolahan informasi yang akan diperbaiki atau digunakan kembali perlu

dipastikan bahwa tidak ada informasi sensitif yang masih terkandung sebelum peralatan tersebut diperbaiki atau digunakan kembali.

14.4. Prosedur terkait dengan disposal dan penggunaan kembali peralatan telah diatur dalam Prosedur Pengelolaan Aset.

# BAB V KENDALI KEAMANAN INFORMASI ASPEK TEKNOLOGI

## 1. PERANGKAT ENDPOINT PENGGUNA

1.1. Pengguna fasilitas notebook harus memperhatikan keamanan data yang disimpan pada perangkat pada saat digunakan di luar area organisasi.

1.2. Fasilitas notebook yang sedang tidak digunakan di luar area organisasi harus dipastikan keamanan fisik untuk mencegah terjadinya pencurian / kehilangan perangkat.

1.3. Penggunaan perangkat mobile (*mobile device*) seperti notebook serta smartphone yang menyimpan informasi milik Diskominfo Kab. Kendal ataupun milik Pihak Eksternal yang telah diserahkan pengelolaannya terhadap Diskominfo Kab. Kendal harus memiliki kontrol keamanan yang baik untuk menangani risiko terhadap kerahasiaan, integritas serta ketersediaannya.

1.4. Perlindungan tersebut dapat mencakup namun tidak terbatas pada perlindungan secara fisik, pengendalian akses ke peralatan perangkat mobile, kriptografi, backup dan perlindungan terhadap malware dan virus.

1.5. Panduan, pelatihan dan program peningkatan kesadaran (*awareness*) perlu dilakukan secara reguler untuk memastikan pemahaman setiap pegawai pengguna fasilitas perangkat mobile akan risiko yang ada serta prosedur pengendalian risiko tersebut.

1.6. Pengguna harus memastikan aset yang sedang tidak digunakan telah terlindungi dengan baik dengan menghentikan (*terminate*) session aktif terhadap sistem setelah selesai digunakan.

1.7. Sedapat mungkin melakukan *log-off* pada komputer atau server setelah session selesai digunakan.

1.8. Mengamankan komputer atau terminal yang digunakan dengan menggunakan password.

## 2. HAK AKSES KHUSUS

2.1. Pemberian dan penggunaan hak akses khusus untuk informasi (*read and write*) dan sistem informasi (root, administrator) organisasi harus dibatasi dan dikendalikan. Yang dimaksud dengan hak akses khusus adalah pemberian hak akses untuk keperluan pemeliharaan dan pengujian sistem, serta audit.

2.2. Proses otorisasi dan catatan dari semua hak akses khusus yang diberikan harus didokumentasikan.

2.3. Hak akses khusus harus diberikan dalam format User ID yang berbeda dengan hak akses biasa dan bersifat sementara.

2.4. Penggunaan hak akses khusus harus dimonitor untuk memastikan tidak adanya akses tanpa izin. Hak akses dengan tujuan untuk pelaksanaan audit terhadap sistem harus diberikan dengan wewenang *read only*.

2.5. Pengelolaan hak akses khusus perlu memperhatikan beberapa hal berikut:

2.5.1. Persetujuan formal untuk hak akses khusus perlu diberikan oleh pemilik dari informasi atau sistem informasi terkait;

2.5.2. Pemantauan/peninjauan secara berkala untuk hak akses khusus yang telah dialokasikan; dan

2.5.3. 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 setelah salah satu pemegang *password* berhenti atau mengalami mutasi.

## 3. PEMBATASAN AKSES INFORMASI

3.1. Akses ke informasi pada sistem jaringan oleh pengguna harus dibatasi sesuai dengan kewenangan akses.

3.2. Pembatasan akses dilakukan berdasarkan kebutuhan personel sesuai dengan keperluan operasional dan bisnis personel tersebut.

*3.3.* Pembatasan akses perlu dilakukan untuk informasi pada sistem informasi. Hal ini dapat dilakukan antara lain dengan pengendalian hak untuk *read, write, copy* maupun *delete.*

## 4. PENGENDALIAN AKSES KE *SOURCE CODE* PROGRAM

4.1. 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.

4.2. Beberapa hal berikut dapat dipertimbangkan dalam pengendalian akses ke *source code* program :

4.2.1. Penyimpanan *source code* tidak dilakukan pada sistem operasional.

4.2.2. Pengendalian akses *source code* perlu diimplementasikan.

4.2.3. Diperlukan proses otorisasi resmi untuk mengakses *source code*.

4.2.4. Daftar *source code* perlu dibuat, dipelihara dan dijaga.

4.2.5. Setiap akses ke *source code* program perlu didokumentasikan, termasuk

audit log untuk akses tersebut.

4.2.6. Pemeliharaan dan penyalinan *source code* program harus dilakukan melalui mekanisme pengendalian perubahan.

## 5. PROSEDUR LOG-ON SECARA AMAN

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

5.1. Tidak memberikan pesan bantuan yang dapat menyebabkan log-on tanpa izin.

5.2. Membatasi jumlah kesalahan dalam percobaan log-on serta melakukan hal-hal berikut apabila jumlah kesalahan maksimal telah terlewati maka hal tersebut perlu dipertimbangkan:

5.2.1. Merekam setiap percobaan log-on baik yang gagal maupun berhasil.

5.2.2. Memberikan jeda waktu sebelum log-on dapat dilakukan kembali atau menolak percobaan kembali setelah terjadi kesalahan dalam percobaan log-on.

5.2.3. Memutuskan koneksi data.

5.2.4. Memberikan pesan peringatan pada sistem bahwa jumlah maksimal percobaan log-on telah terlewati.

5.2.5. Jumlah maksimal percobaan log-on perlu mempertimbangkan panjang minimal dari *password* dan nilai dari sistem yang dilindungi.

5.3. Tidak menampilkan karakter password pada saat log-on. Tampilan karakter password dapat diganti dengan simbol.

5.4. Tidak memberikan petunjuk mengenai sistem atau aplikasi sebelum proses log-on telah sukses dilakukan.

5.5. Menampilkan peringatan, bahwa sistem atau aplikasi hanya boleh diakses oleh orang yang berkepentingan.

5.6. 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.

5.7. Membatasi waktu minimal dan maksimal untuk proses log-on.

5.8. Setelah proses log-on yang berhasil sistem perlu menampilkan waktu dari proses log-on terakhir, baik yang berhasil maupun yang gagal.

5.9. Tidak mentransmisikan *password* dalam *clear text* melalui jaringan.

## 6. MANAJEMEN KAPASITAS

6.1. Setiap penanggung jawab sistem di Diskominfo Kab. Kendal harus melakukan

manajemen kapasitas untuk setiap pengembangan infrastruktur dan sistem aplikasi baru maupun yang sedang berjalan dengan mempertimbangkan proyeksi terhadap kebutuhan operasional, dan infrastruktur berdasarkan kebutuhan bisnis yang akan datang dan sistem informasi organisasi. Selain itu proyeksi tersebut perlu juga mempertimbangkan kondisi sistem informasi organisasi saat ini dan tren proyeksi perkembangan sistem selama ini.

6.2. Pengukuran kapasitas terhadap aplikasi dan infrastruktur dilakukan secara periodik.

6.3. Penggunaan seluruh sumber daya pengolahan informasi dalam sistem informasi organisasi harus dipantau, dilakukan proses *tuning* untuk menjamin kinerja sistem yang diharapkan dapat selalu tersedia dan tidak terjadinya kegagalan sistem karena kapasitas yang tidak mencukupi.

6.4. Semua aktivitas atau proses dalam sistem informasi baik yang sedang berjalan maupun yang akan dijalankan harus mengidentifikasi item kebutuhan kapasitas sistem, sebagai contoh adalah kapasitas memori atau storage dalam server, utilisasi CPU server atau utilisasi backbone jaringan WAN.

6.5. Dalam proses manajemen kapasitas perhatian lebih perlu diberikan untuk sistem atau perangkat pengolahan informasi yang memiliki biaya tinggi secara finansial, waktu maupun penggunaan sumber daya manusia. Untuk sistem dengan biaya tinggi tersebut pemilik atau manajer sistem perlu memantau secara seksama penggunaan dan utilisasi sistem.

6.6. Proses manajemen kapasitas juga perlu mempertimbangkan adanya ketergantungan atau *bottleneck* terkait sumber daya manusia yang dapat menimbulkan ancaman terhadap aspek kerahasiaan, integritas maupun ketersediaan informasi dan sistem informasi organisasi.

## 7. PENGENDALIAN TERHADAP *MALWARE*

7.1. Kontrol terhadap *malware* dapat dilakukan melalui pendeteksian dan pencegahan serangan *malware* dan pemulihan setelah terjadi serangan dari *malware*.

7.2. Pegawai di lingkungan Diskominfo Kab. Kendal harus melindungi sistem informasi dari serangan *malware* dengan tidak meng-install perangkat lunak illegal, dan/atau *unwanted* program.

7.3. Setiap perangkat seperti PC dan Notebook, dan server harus menggunakan antivirus untuk mencegah bahaya *malware (virus, worm, trojan).*

7.4. Setiap pegawai Diskominfo Kab. Kendal 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.

7.5. *Update* dan *scanning* rutin harus dilakukan secara otomatis untuk mendeteksi virus pada komputer dan media penyimpanan. Proses pendeteksian mencakup:

7.5.1. Data dalam media penyimpanan elektronik maupun optik dan data yang diperoleh melalui jaringan komunikasi sebelum digunakan.

7.5.2. *Attachment* dari *e-mail*. Hal ini perlu dilakukan pada beberapa titik dalam sistem informasi seperti *e-mail server,* pada perangkat jaringan dan komputer pengguna.

7.6. Kesadaran (*awareness*) pengguna sistem informasi terhadap bahaya serangan *malware* perlu terus menerus dipelihara.

7.7. Perlindungan sistem informasi dari serangan *malware* dapat dilakukan oleh Diskominfo Kab. Kendal melalui kombinasi dari :

7.7.1. Penggunaan perangkat lunak untuk mendeteksi dan memperbaiki kerusakan yang disebabkan oleh *malware*.

7.7.2. Program peningkatan kesadaran pengguna.

7.7.3. Pengendalian untuk akses ke sistem informasi dan pengelolaan perubahan.

7.8. Beberapa hal berikut perlu diimplementasikan untuk melindungi sistem informasi dari serangan *malware*.

7.8.1. Secara formal melarang penggunaan perangkat lunak yang tidak diizinkan.

7.8.2. Antivirus yang terpasang harus dikonfigurasi untuk beroperasi secara terus-menerus pada sistem TIK. Pengguna dilarang untuk mengubah konfigurasi perangkat lunak antivirus yang terpasang.

7.8.3. Peninjauan berkala harus dilakukan terhadap *software* dan data yang digunakan untuk mendukung proses bisnis untuk memastikan tidak ada data atau perangkat lunak yang tidak diizinkan dalam sistem informasi organisasi.

7.8.4. Apabila tidak memungkinkan untuk dilakukan updating secara otomatis, maka harus terdapat prosedur untuk melakukan proses updating secara manual.

7.8.5. Tindakan yang perlu dilakukan untuk menangani infeksi malware harus didefinisikan, didokumentasikan dan diinformasikan kepada pengguna, antara lain:

- Disket / CD / *flash disk* dan media eksternal lainnya yang diduga terinfeksi virus harus diisolasi.
- Komputer, server, *workstation* yang diduga terinfeksi virus, harus dibersihkan sesegera mungkin.
- Semua kejadian yang berkaitan dengan virus harus dilaporkan ke

organisasi dan di *log* sebagai insiden pengamanan (*security incident*).

7.8.6. Penggunaan perangkat lunak untuk pengendalian malware perlu dilengkapi dengan pengaktifan fungsi update secara otomatis.

## 8. PENGENDALIAN TERHADAP KELEMAHAN TEKNIS (*TECHNICAL VULNERABILITY*)

8.1. Perubahan Sistem Operasi pada server sistem informasi Diskominfo Kab. Kendal harus dilakukan pengujian agar tidak mengganggu kelangsungan operasional yang mencakup kepastian keandalan sistem informasi.

8.2. Informasi mengenai kelemahan dari sistem informasi Diskominfo Kab. Kendal harus diperoleh tepat waktu. Informasi tersebut tidak boleh terungkap ke pihak lain dan juga perlu dikendalikan melalui proses *risk assessment*.

8.3. Inventarisasi dari aset informasi yang lengkap dan terkini merupakan syarat utama dari proses manajemen yang efektif dari kelemahan teknis. Informasi spesifik yang diperlukan untuk mendukung proses manajemen ini mencakup vendor perangkat lunak, versi perangkat lunak, status dari penggunaan serta pegawai yang bertanggung jawab untuk perangkat lunak tersebut.

8.4. Tindakan yang cepat perlu diambil terhadap adanya potensi kelemahan teknis. Hal-hal berikut perlu dipertimbangkan untuk memastikan efektivitas proses manajemen dari kelemahan teknis :

8.4.1. Identifikasi dari sumber daya yang dibutuhkan untuk mengidentifikasi kelemahan teknis dari perangkat pengolah informasi yang telah diinventarisasi dan untuk menjaga *awareness* tentang kelemahan tersebut.

8.4.2. Jangka waktu penanganan kelemahan teknis maupun potensinya yang diidentifikasikan harus dibuat.

8.4.3. Setelah kelemahan teknis tersebut telah diidentifikasi, organisasi perlu mengambil tindakan berdasarkan identifikasi risiko yang muncul dari kelemahan tersebut.

8.4.4. Perubahan untuk mengatasi kelemahan tersebut perlu dilaksanakan berdasarkan proses pengelolaan perubahan dan penanganan insiden keamanan informasi.

8.4.5. Dalam melakukan *patching* untuk mengatasi kelemahan teknis, perlu dilakukan analisa risiko untuk membandingkan risiko antara kelemahan teknis yang ada sebelum dan sesudah proses instalasi *patch*.

8.4.6. *Patch* yang ada perlu diuji dan dievaluasi sebelum di-install 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.

8.4.7. Apabila *patch* untuk mengatasi kelemahan teknis tersebut tidak ada maka pengendalian berikut dapat dipertimbangkan :

- Mematikan layanan atau perangkat sistem informasi yang memiliki dan/atau terkait dengan kelemahan teknis tersebut.
- Mengubah atau menambah kontrol akses, seperti *access control list* di firewall.
- Meningkatkan monitoring sistem untuk mendeteksi atau mencegah adanya eksploitasi dari kelemahan teknis tersebut.
- Meningkatkan kesadaran akan adanya kelemahan teknis tersebut.
- Pemeliharaan audit log untuk semua prosedur yang terkait dengan kelemahan teknis tersebut.
- Pengawasan dan evaluasi secara reguler proses manajemen kelemahan teknis tersebut untuk menjamin efektivitas dan efisiensi.
- Memberikan prioritas pertama perlu diberikan untuk sistem dengan risiko tinggi.

## 9. MANAJEMEN KONFIGURASI

9.1. Inventarisasi aset IT yang digunakan dalam infrastruktur mencakup perangkat keras, perangkat lunak, sistem operasi, aplikasi, serta perangkat jaringan yang digunakan yang membantu dalam pengelolaan konfigurasi dan pemantauan keamanan

9.2. Pengelolaan perubahan konfigurasi meliputi evaluasi perubahan yang diajukan, pengujian perubahan dan pemantauan dampak dari perubahan konfigurasi terhadap keamanan dan kinerja sistem

9.3. Penerapan prinsip hak akses berlaku untuk akses yang diperlukan sehingga mencegah penyalahgunaan akses

9.4. Audit terhadap *Configuration Item* (CI) dilakukan untuk memverifikasi kepatuhan terhadap standar konfigurasi dan kebijakan organisasi sekurangnya sekali dalam setahun.

## 10. PENGHAPUSAN INFORMASI

10.1. Pedoman terkait dengan masa retensi dan penghapusan informasi untuk semua korespondensi bisnis perlu mempertimbangkan peraturan perundang-undangan dan regulasi yang berlaku.

10.2. Penggunaan media penyimpanan elektronis perlu mempertimbangkan metode khusus untuk menjamin bahwa media penyimpanan elektronis tersebut dapat diakses selama masa retensi informasi tersebut.

10.3. Sistem penyimpanan dan penanganan informasi harus memiliki sistem identifikasi masa retensi sesuai dengan hukum, regulasi dan aturan negara yang berlaku. Hal ini perlu dilakukan terutama apabila informasi yang disimpan merupakan bukti kepatuhan terhadap hukum, regulasi dan aturan negara yang berlaku. Sistem ini juga harus memungkinkan penghancuran informasi organisasi setelah masa retensi telah terlewat dan informasi tersebut tidak lagi dibutuhkan.

10.4. Penghapusan informasi dari media penyimpanan elektronik dapat dilakukan dengan metode format ulang, penghancuran media, atau dengan metode *degaussing* (magnetisasi).

## 11. 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.

11.1. Identifikasi Data Sensitif merupakan langkah pertama untuk mengidentifikasi jenis data sensitif yang perlu dilindungi, seperti nomor kartu kredit, data medis, atau informasi identifikasi pribadi (PII). Hal ini penting untuk memahami jenis data yang harus di-mask dan melindunginya dengan tepat.

11.2. Penentuan Metode Masking yang sesuai harus ditentukan. Metode yang digunakan meliputi :

11.2.1. Substitusi Karakter: 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'.

11.2.2. Pertukaran Nilai: 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.

11.2.3. Pembuatan Data Palsu: 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.

11.3. Implementasi 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 masking.

## 12. 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 sensitive.

12.1. Identifikasi data sensitif yang perlu dilindungi melalui mekanisme klasifikasi informasi. Informasi tersebut termasuk data pribadi dan informasi rahasia perusahaan.

12.2. 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 dalam perusahaan serta pengiriman data melalui jaringan internal dan eksternal.

12.3. Identifikasi dan Pengawasan Data menggunakan Teknologi DLP untuk mengidentifikasi dan memonitor data sensitif. Teknologi DLP dapat memindai data dalam berbagai bentuk seperti dokumen, email, 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.

12.4. 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.

12.5. 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 yang berlaku.

12.6. 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.

## 13. BACKUP INFORMASI

13.1. Informasi elektronis yang bersifat rahasia atau kritikal (memiliki tingkat integritas dan ketersediaan tinggi) harus memiliki Backup, sehingga dalam hal data/informasi utama tidak dapat dibaca, rusak, dan lain sebagainya, masih dapat menggunakan data Backup.

13.2. Frekuensi dan tingkat Backup (penuh atau parsial) disesuaikan dengan kebutuhan kritikalitas bisnis.

13.3. Hasil Backup harus disimpan pada tempat yang aman dan diusahakan ditempatkan di luar lokasi utama dan diberikan perlindungan secara fisik dan lingkungan yang memadai.

13.4. Media Backup harus diuji secara berkala melalui uji restore untuk memastikan media tersebut dapat berfungsi dengan baik pada saat dibutuhkan.

13.5. Masa retensi dari Backup informasi tergantung dari tingkat kritikalitas suatu informasi dan sistem yang dioperasikan di Diskominfo Kab. Kendal

13.6. Informasi yang dimiliki organisasi harus secara rutin di-*Backup* sesuai dengan kebijakan dan strategi Backup formal organisasi.

13.7. Fasilitas Backup yang memadai harus disediakan untuk memastikan bahwa proses pemulihan (*recovery*) dapat dilakukan untuk semua informasi dan perangkat lunak yang dibutuhkan apabila terjadi gangguan atau bencana.

13.8. Beberapa hal berikut perlu dipertimbangkan dalam proses *Backup* informasi :

13.8.1. Informasi yang perlu di-Backup harus ditentukan.

13.8.2. Daftar informasi yang telah di-Backup harus didokumentasikan dalam sebuah record yang harus selalu dipelihara.

13.8.3. Prosedur *restore* harus diuji secara berkala untuk memastikan *restore* dapat dilakukan secara efektif dan dapat selesai dilakukan dalam jangka waktu yang telah ditentukan.

13.8.4. Informasi yang bersifat sensitif perlu menggunakan pengamanan berupa enkripsi pada *Backup*-nya.

## 14. KETERSEDIAAN DARI FASILITAS PEMROSESAN INFORMASI

14.1. Diskominfo Kab. Kendal harus memastikan fasilitas pemrosesan jaringan mempunyai *redundancy* yang cukup terhadap layanan jaringan yang diberikan untuk memenuhi kebutuhan ketersediaan sistem.

14.2. Apabila kebutuhan *redundancy* tidak dapat dipenuhi. Maka, proses alternatif perlu dilakukan untuk memastikan ketersediaan dari proses bisnis dan operasional.

14.3. Fasilitas pengolahan informasi beserta sarana pendukungnya yang telah memenuhi

aspek *redundancy* harus diuji secara berkala untuk menjamin kesesuaian dari fungsinya.

## 15. LOGGING

15.1. Log audit harus direkam dan disimpan pada sistem untuk memantau aktivitas pengguna dalam jangka waktu yang ditentukan.

15.2. Log audit yang perlu disimpan mencakup pada aspek berikut:

15.2.1. User ID Tanggal dan waktu serta detail dari kejadian penting (*key events*) dalam sistem seperti *log-on* dan *log-off*.

15.2.2. Records untuk percobaan akses baik yang berhasil maupun gagal.

15.2.3. Ide Perubahan pada konfigurasi sistem.

15.2.4. Penggunaan hak akses khusus (*privilege*).

15.2.5. Data yang diakses dan jenis dari akses tersebut.

15.2.6. Alamat dan protokol jaringan.

15.2.7. Peringatan alarm yang dibuat oleh sistem pengendalian akses.

15.2.8. Pengaktifan dan penonaktifan dari sistem pengamanan seperti sistem antivirus atau *intrusion detection system* dari terminal atau komputer.

15.3. Event Log yang digunakan untuk merekam aktivitas pengguna, pengecualian (*exception*), kegagalan (*fault*), dan kejadian keamanan informasi harus dibuat dan dipelihara dalam jangka waktu paling tidak 7 (tujuh) hari untuk membantu penyelidikan di masa mendatang dan pengawasan pengendalian akses.

15.4. Log audit dapat berisi informasi yang bersifat sensitif. Sehingga klasifikasinya dan pengamannya perlu disesuaikan.

15.5. Log sistem harus dilindungi dari modifikasi dan akses tanpa izin yaitu pembatasan terhadap perubahan atau penghapusan terhadap log files.

15.6. Administrator sistem harus memastikan kapasitas penyimpanan dari log files untuk menghindari penyimpanan yang penuh yang dapat menyebabkan kegagalan dalam untuk mencatat kejadian (*event*) atau *overwriting* kejadian (*event*) yang lama.

15.7. Penyimpanan audit log perlu mempertimbangkan masa retensi yang telah ditentukan dan kebutuhan untuk pengumpulan bukti audit.

15.8. Seluruh aktivitas administrator dan operator sistem informasi harus direkam dalam log dan ditinjau secara berkala yang mencakup :

15.8.1. Waktu dari kejadian (event) baik yang sukses maupun gagal.

15.8.2. Hak akses dan identitas dari administrator atau operator.

15.8.3. Informasi mengenai kejadian (event) atau kegagalan yang terjadi.

15.8.4. Proses yang sedang berjalan saat kejadian (*event*) terjadi.

15.9. Log bagi administrator dan operator sistem harus ditinjau secara rutin.

## 16. AKTIVITAS PEMANTAUAN

16.1. Diskominfo Kab. Kendal perlu menerapkan aktivitas pemantauan terhadap aset teknologi informasi. Sistem pemantauan yang dilakukan meliputi:

16.1.1. Jaringan keluar dan masuk, lalu lintas sistem dan aplikasi;

16.1.2. Akses ke sistem, server, peralatan jaringan, sistem pemantauan, dan aplikasi penting

16.1.3. Sistem tingkat kritis atau admin dan file konfigurasi jaringan;

16.1.4. Log dari alat keamanan [misal. antivirus, IDS, sistem pencegahan intrusi (IPS), filter web, firewall, pencegahan kebocoran data];

16.1.5. Log peristiwa yang berkaitan dengan aktivitas sistem dan jaringan

16.1.6. Memeriksa bahwa kode yang sedang dieksekusi diizinkan untuk berjalan di sistem dan belum dirusak (misalnya dengan kompilasi ulang untuk menambahkan kode tambahan yang tidak diinginkan);

16.1.7. Penggunaan sumber daya (misalnya CPU, hard disk, memori, bandwidth) dan kinerjanya.

16.2. Sistem pemantauan yang dilakukan bertujuan untuk mengidentifikasi perilaku anomali, seperti :

16.2.1. Penghentian proses atau aplikasi yang tidak direncanakan;

16.2.2. Aktivitas yang biasanya terkait dengan malware atau lalu lintas yang berasal dari alamat IP berbahaya atau domain jaringan yang diketahui

16.2.3. Karakteristik serangan yang diketahui (seperti *denial of service*)

16.2.4. Perilaku sistem yang tidak biasa

16.2.5. *Bottleneck* dan *overload* jaringan

16.2.6. Akses tidak sah ke sistem atau informasi;

16.2.7. Pemindaian aplikasi, sistem, dan jaringan bisnis yang tidak sah;

16.2.8. Perilaku pengguna dan sistem yang tidak biasa dalam kaitannya dengan perilaku yang diharapkan.

16.3. Kejadian abnormal yang didapat harus dikomunikasikan kepada pihak terkait untuk dilakukan tindakan. Temuan dari kejadian abnormal akan ditindak mengikuti prosedur manajemen insiden keamanan informasi.

## 17. SINKRONISASI WAKTU

17.1. *Clock* dari seluruh sistem pengolahan informasi dalam organisasi atau sebuah domain jaringan informasi harus disinkronisasi.

17.2. Sistem pengolahan informasi seperti server yang memiliki fungsi *real time clock* maka waktu tersebut harus disinkronisasikan dengan sebuah standar waktu.

17.3. 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.

17.4. Sinkronisasi *clock* perlu diimplementasikan untuk menjamin akurasi dari *log* audit.

## 18. PENGGUNAAN PROGRAM UTILISASI KHUSUS.

18.1. Penggunaan *system utility programs* yang berpotensi dapat mengambil alih pengendalian sistem jaringan harus dibatasi dan dikendalikan secara ketat.

18.2. Administrator Jaringan harus melakukan proses identifikasi, otentifikasi dan otorisasi untuk seluruh *system utilities* yang digunakan dan membatasi penggunaan *system utilities*.

18.3. Contoh dari system utility tersebut adalah aplikasi yang memiliki akses ke registry sistem operasi atau aplikasi yang memiliki akses langsung untuk memanipulasi database.

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

## 19. INSTALASI DAN PEMBATASAN PERANGKAT LUNAK PADA SISTEM OPERASIONAL

19.1. Diskominfo Kab. Kendal harus mengendalikan instalasi software pada sistem operasional (*production*)

19.2. Pengendalian terhadap sistem operasional meliputi :

19.2.1. Sistem production hanya mengoperasikan sistem yang telah disetujui oleh Kepala Diskominfo Kab. Kendal dan tidak boleh digunakan untuk menjalankan aplikasi yang masih dalam tahap pengembangan.

19.2.2. Konfigurasi sistem operasional harus didokumentasikan dan di-update setiap kali mengalami perubahan.

19.2.3. Proses updating perangkat lunak, aplikasi dan library pada sistem production hanya boleh dilakukan oleh pegawai yang diberi wewenang setelah mendapatkan otorisasi dari pihak manajemen.

19.2.4. Aplikasi dan sistem operasi dapat di-install pada sistem production setelah dengan sukses diuji. Pengujian tersebut dilakukan pada sistem selain sistem production dan mencakup namun tidak terbatas pada pengujian fungsi,

kegunaan, keamanan serta dampak terhadap sistem lain.

19.2.5. Sistem pengendalian konfigurasi harus digunakan untuk memonitor dan mengendalikan seluruh aplikasi yang di-install pada sistem production beserta dokumentasinya.

19.2.6. Sebuah strategi rollback harus dibuat sebelum setiap perubahan pada sistem production dilakukan.

19.2.7. Audit log harus dipelihara untuk semua update pada sistem production.

19.2.8. Versi lama dari aplikasi yang telah di-install pada sistem production harus disimpan.

19.2.9. Versi lama dari aplikasi perlu disimpan, bersama dengan dokumentasi sistem aplikasi tersebut yang mencakup namun tidak terbatas pada parameter, prosedur, konfigurasi serta aplikasi pendukung lainnya.

19.3. Dukungan dari vendor penyedia aplikasi perlu dipastikan untuk jangka waktu di mana aplikasi tersebut masih digunakan pada sistem production.

19.4. Setiap keputusan untuk melakukan upgrade aplikasi perlu mempertimbangkan kebutuhan bisnis serta keamanan informasi pada versi yang baru. Upgrade tidak boleh dilakukan hanya atas dasar pertimbangan bahwa upgrade tersebut ada.

19.5. Akses secara fisik maupun logikal dapat diberikan kepada pihak vendor apabila diperlukan untuk keperluan pemeliharaan sistem dan/atau aplikasi. Akses ini perlu mendapat persetujuan manajemen dan aktivitas vendor tersebut harus diawasi.

19.6. Perubahan atau modifikasi perangkat lunak harus dikendalikan untuk memastikan kelangsungan layanan jaringan.

19.7. Perangkat lunak yang digunakan harus berlisensi resmi dan sesuai dengan aturan keamanan informasi yang ada di Diskominfo Kab. Kendal

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

19.9. Instalasi perangkat lunak harus dilakukan oleh administrator sistem terkait.

## 20. KEAMANAN JARINGAN

20.1. Akses ke jaringan eksternal ke data center Diskominfo Kab. Kendal dapat dilakukan dengan sangat terbatas dan dengan menggunakan perangkat komputer yang terpisah dari jaringan Diskominfo Kab. Kendal

20.2. Dalam penggunaan *shared network*, hak akses pengguna untuk mengakses jaringan informasi Diskominfo Kab. Kendal yang dikelola oleh Diskominfo Kab. Kendal harus dibatasi sesuai dengan pengendalian akses.

20.3. Jaringan perlu dikelola dan dikendalikan untuk melindungi informasi dan sistem

informasi yang terdapat di dalamnya.

20.4. Secara khusus hal berikut perlu dipertimbangkan:

20.4.1. Apabila memungkinkan, personel yang bertanggung jawab untuk operasional jaringan harus dipisahkan tanggung jawabnya dari operasional komputer dan server.

20.4.2. Prosedur pengaksesan jaringan menggunakan perangkat akses remote harus diatur dengan jelas.

20.4.3. Kontrol khusus harus diterapkan untuk menjaga kerahasiaan dan integritas informasi yang dikirimkan melalui jaringan publik dan wireless.

20.4.4. Manajemen jaringan (*network management*) dilakukan secara terkontrol dan konsisten yang meliputi *logging, monitoring, incident response* dan *network traffic management*.

20.4.5. 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.

20.4.6. Akses ke jaringan organisasi harus dibatasi dan setiap akses perlu diotentikasi sebelum dapat diberikan akses ke jaringan.

20.4.7. Penggunaan perangkat pengamanan jaringan komunikasi, yang mencakup namun tidak terbatas pada firewall, Intrusion Detection System (IDS), dan Intrusion Prevention System (IPS).

20.4.8. Pengujian secara berkala terhadap keamanan jaringan komunikasi, misalnya dengan *penetration testing*.

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

## 21. KEAMANAN LAYANAN JARINGAN

21.1. Fitur keamanan, tingkat layanan dan kebutuhan terhadap layanan jaringan yang diidentifikasi dalam operasional sistem di Diskominfo Kab. Kendal harus dimonitor dan dievaluasi secara berkala.

21.2. Layanan jaringan mencakup seluruh layanan dari sistem informasi Diskominfo Kab. Kendal yang menggunakan jaringan komunikasi dalam operasionalnya, seperti e-mail, internet dan layanan aplikasi organisasi antarcabang atau aplikasi *enterprise resource planning* antarkantor.

21.3. Fungsi keamanan, tingkat layanan dan *requirement* dari manajemen untuk semua layanan jaringan harus diidentifikasi dalam seluruh perjanjian layanan jaringan, tanpa memandang apakah layanan jaringan diberikan oleh pihak internal maupun eksternal.

21.4. 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.

21.5. Teknologi pengamanan layanan jaringan dapat berupa otentifikasi, enkripsi dan pengendalian koneksi jaringan.

## 22. PEMISAHAN (SEGREGATION) DALAM JARINGAN

22.1. Jaringan yang disediakan bagi kelompok (group) untuk layanan informasi, user, dan sistem informasi harus dipisahkan.

22.2. Segmentasi pada jaringan internal dilaksanakan oleh Diskominfo Kab. Kendal berdasarkan kebutuhan operasional Diskominfo Kab. Kendal dan sensitivitas dari sistem.

22.3. Hal tersebut dilakukan dengan membagi jaringan tersebut menjadi domain jaringan yang terpisah, baik secara fisik maupun logikal.

22.4. Pemisahan yang pertama kali perlu dilakukan adalah memisahkan antara domain jaringan internal dengan jaringan eksternal organisasi.

22.5. Pemisahan tersebut membutuhkan penilaian risiko yang menyeluruh untuk menganalisis kebutuhan keamanan informasi dari masing-masing domain yang ada dan untuk pengaturan akses dan arus informasi antardomain jaringan.

22.6. Pemisahan dalam jaringan tersebut dapat diimplementasikan dengan antara lain:

22.6.1. Pemasangan *secure gateways* seperti firewall antara domain jaringan untuk mengatur akses dan arus informasi dengan cara melakukan *traffic filtering* antardomain jaringan.

22.6.2. Mengimplementasikan virtual LAN untuk setiap domain atau group pengguna sistem informasi organisasi.

22.6.3. Pemisahan jaringan perlu dilakukan untuk memisahkan jaringan wireless organisasi dengan dilengkapi dengan kontrol keamanan seperti metode kriptografi serta otentifikasi.

## 23. WEB FILTERING

23.1. Diskominfo Kab. Kendal harus mengurangi risiko personelnya mengakses situs web yang berisi informasi ilegal atau diketahui mengandung virus atau phishing.

23.2. 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

23.3. Pemblokiran penggunaan aplikasi yang digunakan untuk mengakses situs berbahaya

dan ilegal

23.4. Pertimbangan blokir IP dan domain web dengan kriteria:

23.4.1. Situs web yang memiliki fungsi pengunggahan informasi kecuali diizinkan untuk alasan bisnis yang sah;

23.4.2. Situs web berbahaya yang diketahui atau dicurigai yang diperoleh dari aktivitas *threat intelligence* (situs web yang mendistribusikan *malware* atau konten *phishing*);

23.4.3. Situs web berbagi konten ilegal.

## 24. PENGGUNAAN KRIPTOGRAFI

24.1. 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 oleh organisasi.

24.2. Penggunaan teknologi kriptografi dapat digunakan untuk melindungi informasi milik Diskominfo Kab. Kendal

24.3. Keputusan penggunaan teknologi kriptografi perlu menimbang sensitivitas (sisi kerahasiaan) dan kritikalitas (sisi integritas) dari informasi yang akan dilindungi.

24.4. Penggunaan enkripsi harus dipertimbangkan untuk melindungi informasi sensitif dan/atau rahasia yang dipindahtangankan atau dikirimkan baik melalui media jaringan informasi maupun transportasi secara fisik menggunakan removable media atau *device*.

24.5. Implementasi kriptografi perlu mempertimbangkan aspek hukum dan regulasi negara, yang mungkin membatasi penggunaan kriptografi terutama untuk pengiriman data antarnegara.

24.6. Proses pengembangan sistem aplikasi yang mengolah informasi rahasia harus menerapkan pengamanan terhadap informasi yang dihasilkan dan dipertukarkan sehingga terhindar dari akses ilegal dan pencurian informasi oleh pihak-pihak tertentu, salah satunya adalah dengan menerapkan enkripsi yang andal.

24.7. Enkripsi diterapkan untuk memastikan keamanan informasi rahasia dalam proses pertukarannya pada area mobile dan desktop computing, sistem jaringan, sistem e-mail, removable media dan pembangunan sistem aplikasi.

24.8. Pertukaran informasi rahasia yang menggunakan media e-mail harus memenuhi hal berikut:

24.8.1. Menerapkan enkripsi dalam mengamankan isi serta *attachment e-mail* agar tidak dapat dibaca oleh pihak yang tidak berwenang.

24.8.2. Menerapkan *message integrity check* untuk memastikan isi berserta attachment e-mail tidak diubah oleh pihak yang tidak berwenang selama dalam perjalanan.

24.8.3. Menerapkan *digital signature* untuk menghindari penolakan (*repudiation).*

24.9. Enkripsi harus diterapkan untuk melindungi data yang berasal dari *production system* dan bersifat rahasia sebelum digunakan sebagai testing data di *environment UAT*. Penggunaan data *scrambling* dapat digunakan sebagai alternatif dalam melindungi kerahasiaan data asli sebelum digunakan sebagai data testing.

24.10. Tidak disarankan menggunakan proprietary enkripsi yang belum teruji keandalannya.

24.11. Enkripsi yang disarankan untuk diterapkan dalam penyimpanan informasi yang bersifat rahasia adalah dengan panjang key minimal 256 bit. Algoritma yan digunakan misalnya:

24.11.1. *Advanced Encryption Standard* (AES);

24.11.2. 3DES; atau

24.11.3. Algoritma lainnya yang menggunakan panjang *key* minimal 256 bit.

24.12. Pada sistem aplikasi web based, apabila enkripsi belum dapat diterapkan, maka harus diterapkan enkripsi pada protokol komunikasi berupa SSL/HTTPS.

24.13. Sistem aplikasi yang ada sebelum terbitnya kebijakan ini dan belum memiliki fitur enkripsi untuk penyimpanan atau pertukaran informasi, maka perlu dilakukan review/asesmen risiko oleh pemilik sistem aplikasi bersama Unit Pengembangan terkait. Review ini selain menentukan klasifikasi informasinya, juga untuk mengidentifikasi kontrol pengamanan yang terpasang. Jika kontrol pengamanan yang ada dipandang belum cukup, maka perlu diterapkan kontrol tambahan *(compensating control)* yang memadai atau penerapan fitur enkripsi.

24.14. Seluruh key kriptografi harus dilindungi dari modifikasi, kehilangan serta kerusakan.

24.15. Sistem manajemen dari key kriptografi perlu berdasar pada mekanisme pengelolaan key yang memadai.

24.16. Peralatan yang digunakan untuk menghasilkan dan menyimpan key kriptografi harus dilindungi secara fisik.

24.17. 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.

24.18. Apabila terdapat indikasi kebocoran key kriptografi, maka key tersebut harus segera dicabut dan diganti.

## 25. KEBIJAKAN KEAMANAN DALAM PENGEMBANGAN SISTEM INFORMASI

25.1. Diskominfo Kab. Kendal harus menetapkan dan mengimplementasikan aturan untuk memastikan keamanan dalam proses pengembangan dan pemberian dukungan (*support*) sistem informasi.

25.2. Aturan tersebut perlu mempertimbangkan:

25.2.1. Pengamanan dari lingkungan pengembangan, seperti pemisahan lingkungan pengembangan baik secara fisik dan/atau logical.

25.2.2. Pengendalian akses.

25.2.3. Panduan keamanan dalam melakukan *coding*

25.2.4. Pengendalian versi aplikasi.

25.2.5. Penyimpanan dari *source code*.

25.2.6. Metode pengujian untuk mengidentifikasi dan memperbaiki *vulnerability*. Jika pengembangan *software* dan sistem menggunakan metode alih daya (*outsourced*). Maka, harus memperhatikan:

- Perjanjian terkait lisensi dan kepemilikan sistem
- Pengujian terhadap penerimaan sistem
- Prasyarat dokumentasi untuk sistem
- Perjanjian *escrow*
- Hak melakukan audit pada proses pengembangan dan kontrol yang diimplementasikan oleh vendor.

## 26. PERSYARATAN KEAMANAN SISTEM INFORMASI

26.1. Setiap perubahan sistem baru maupun perbaikan sistem yang sudah ada harus mempertimbangkan kebutuhan pengendalian keamanan.

26.2. Untuk sistem yang disediakan melalui vendor penyedia, Diskominfo Kab. Kendal perlu melakukan proses pengujian untuk menjamin terpenuhinya seluruh kebutuhan keamanan dalam sistem informasi.

26.3. Proses pengujian dan akuisisi ini perlu mempertimbangkan fungsi keamanan sistem informasi yang disediakan serta risiko yang mungkin muncul dalam penggunaan sistem informasi dari vendor tertentu.

26.4. Penyusunan spesifikasi kebutuhan keamanan informasi perlu memperhatikan implementasi kontrol keamanan. Hal ini perlu dilakukan untuk setiap perangkat lunak untuk aplikasi bisnis dan penunjangnya.

26.5. Kebutuhan keamanan dalam sistem informasi perlu mempertimbangkan kebutuhan dan risiko dari bisnis serta dampak yang mungkin muncul dari kegagalan keamanan

dalam sistem informasi.

26.6. Penyusunan spesifikasi kebutuhan keamanan dalam sistem informasi harus dilakukan pada fase awal pengembangan sistem informasi. Hal ini untuk memastikan kemudahan implementasi keamanan dalam sistem informasi.

26.7. Informasi yang digunakan oleh sistem aplikasi yang dikirimkan melalui jaringan publik harus diamankan untuk menghindari dispute, kebocoran dan perubahan tanpa izin.

26.8. Pengamanan tersebut perlu mempertimbangkan aspek-aspek berikut :

26.8.1. Memastikan identitas dari pihak-pihak yang terlibat dalam pertukaran informasi melalui aplikasi pada jaringan publik;

26.8.2. Memastikan integritas dari informasi yang dipertukarkan;

26.8.3. Memastikan kerahasiaan dari informasi yang dipertukarkan;

26.8.4. Memastikan tidak terjadinya duplikasi dari informasi yang dipertukarkan.

26.8.5. Penggunaan teknologi otentikasi dan enkripsi yang memadai untuk proses pengamanan informasi tersebut.

26.8.6. Pengamanan yang diimplementasikan perlu selaras dengan sensitivitas informasi yang dipertukarkan dan risiko yang ada.

26.8.7. Informasi yang dipertukarkan oleh sistem aplikasi harus diamankan untuk mencegah risiko transmisi yang tidak lengkap, kebocoran, perubahan dan perulangan informasi tanpa otorisasi.

26.8.8. Penggunaan teknologi otentikasi dan enkripsi yang memadai untuk proses pengamanan informasi dan jalur komunikasi yang digunakan untuk pertukaran tersebut harus dipertimbangkan.

26.8.9. Pengamanan yang diimplementasikan perlu selaras dengan sensitivitas informasi yang dipertukarkan dan risiko yang ada.

## 27. REKAYASA SISTEM INFORMASI YANG AMAN

27.1. Diskominfo Kab. Kendal harus menetapkan, mendokumentasikan, memelihara, dan mengimplementasikan fitur-fitur keamanan dalam melakukan rekayasa sistem informasi agar menghasilkan sebuah sistem yang aman.

27.2. Fitur keamanan tersebut harus diimplementasikan pada seluruh komponen dari sistem informasi yang mencakup namun tidak terbatas pada perangkat keras, perangkat lunak, sistem operasi, database pada middleware.

27.3. Pemilihan fitur keamanan sistem informasi tersebut harus dilakukan berdasarkan proses assessment risiko dengan memperhitungkan sensitivitas dan kritikalitas sistem dan informasi yang diproses.

27.4. Fitur keamanan yang perlu dipertimbangkan mencakup namun tidak terbatas pada:

27.4.1. Metode otentikasi pengguna;

27.4.2. Metode pengamanan komunikasi dan session sistem;

27.4.3. Metode untuk validasi informasi;

27.4.4. Metode pengamanan informasi yang diproses dan/atau dipertukarkan oleh sistem berdasarkan sensitivitas dan kritikalitasnya.

## 28. 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 dapat diterapkan meliputi:

28.1. Semua input 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).

28.2. 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.

28.3. 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*.

28.4. *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.

28.5. 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 analisis kode statis.

28.6. 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.

## 29. PENGUJIAN KEAMANAN SISTEM INFORMASI

29.1. Diskominfo Kab. Kendal dan/atau unit kerja yang mengembangkan aplikasi wajib melakukan pengujian sistem informasi, baik dalam proses pengembangan baru maupun *upgrade sistem*.

29.2. Pengujian dilakukan untuk memastikan seluruh prasyarat terkait fitur keamanan informasi yang telah ditetapkan, telah berfungsi sesuai dengan harapan.

29.3. Pengujian keamanan sistem informasi harus dilakukan oleh personel yang memiliki kompetensi untuk melakukan hal tersebut.

29.4. Pengujian penerimaan sistem harus ditetapkan sesuai dengan kriteria sistem informasi baru, upgrade dan versi baru. Pengujian penerimaan sistem harus mencakup pengujian kebutuhan keamanan informasi dan kepatuhan untuk mengamankan pengembangan sistem.

29.5. Pengujian juga harus dilakukan pada komponen yang diterima dan sistem terpadu.

29.6. Seluruh *requirement* dan kriteria penerimaan sistem baru harus didefinisikan dengan jelas, disetujui, didokumentasikan, dan diuji.

29.7. Migrasi sistem dari lingkungan pengembangan ke lingkungan production hanya dapat dilakukan setelah melalui proses pengujian dan penerimaan sistem yang formal. Terkait dengan proses pengujian dan penerimaan sistem, hal-hal berikut harus diperhatikan:

29.7.1. Spesifikasi kebutuhan dan kinerja infrastruktur sistem informasi.

29.7.2. Prosedur untuk pemulihan dari kegagalan (*error recovery*), *restart*, serta rencana dalam kondisi darurat (*contingency plan*).

29.7.3. Persiapan dan pengujian prosedur/manual operasional.

29.7.4. Keterlibatan pengguna dalam pengujian sistem.

29.7.5. Persetujuan formal untuk penerimaan hasil pengujian sistem informasi.

29.7.6. Pelatihan untuk penggunaan sistem baru.

## 30. PENGEMBANGAN PERANGKAT LUNAK SECARA OUTSOURCE

30.1. Pengembangan software yang dilakukan oleh Pihak Ketiga harus diawasi dan dipantau organisasi.

30.2. Pengembangan perangkat lunak secara *outsource* perlu mempertimbangkan beberapa hal berikut :

30.2.1. Kesepakatan mengenai lisensi, kepemilikan *source code* serta hak atas kekayaan intelektual.

30.2.2. Sertifikasi mengenai kualitas dan akurasi dari pekerjaan pengembangan yang dilakukan.

30.2.3. Kesepakatan mengenai *escrow* apabila terjadi kesalahan atau kegagalan pada pekerjaan pengembangan oleh Pihak Ketiga.

30.2.4. Hak untuk melakukan audit terhadap kualitas dan akurasi pekerjaan yang dilakukan.

30.2.5. Syarat dalam kontrak mengenai kualitas dan keamanan dari aplikasi.

30.2.6. Serangkaian pengujian sebelum instalasi dilakukan untuk mendeteksi *malicious code.*

## 31. PEMISAHAN LINGKUNGAN PENGEMBANGAN, PENGUJIAN, DAN OPERASIONAL

31.1. Fasilitas sistem pengembangan, pengujian dan operasional di Diskominfo Kab. Kendal harus dipisahkan untuk mengurangi risiko akses atau perubahan tanpa izin/tidak disengaja pada sistem operasional.

31.2. Tingkat pemisahan antara lingkungan pengembangan, pengujian dan operasional harus diidentifikasi dan pengendalian untuk menjamin terjaganya pemisahan tersebut harus diterapkan.

31.3. Hal-hal berikut perlu dipertimbangkan dalam proses pemisahan tersebut:

31.3.1. Perangkat lunak atau aplikasi yang digunakan untuk lingkungan pengembangan dan operasional harus dijalankan pada sistem atau perangkat keras yang terpisah. Pemisahan tersebut dapat dilakukan secara fisik maupun secara logical.

31.3.2. *Compiler, editor,* dan *tools* pengembangan lain tidak diperbolehkan untuk diakses dari sistem operasional kecuali sangat dibutuhkan.

31.3.3. Apabila memungkinkan lingkungan pengujian harus memiliki kesamaan, baik dari sisi konfigurasi maupun spesifikasi, dengan lingkungan operasional.

31.3.4. Pengguna harus menggunakan profil pengguna yang berbeda ketika menjalankan sistem pada lingkungan operasional dan pengujian.

31.3.5. Menu-menu dalam aplikasi harus menampilkan keterangan yang jelas untuk meminimalkan kesalahan pengguna dalam membedakan lingkungan sistem yang ada.

31.3.6. Data-data yang bersifat sensitif tidak diperbolehkan disalin (*copy*) ke lingkungan pengujian tanpa pengamanan yang memadai.

31.4. Diskominfo Kab. Kendal harus mengamankan lingkungan yang digunakan untuk pengembangan sistem informasi organisasi dalam setiap tahap pada siklus pengembangan.

31.5. Prinsip dalam menetapkan keamanan lingkungan tersebut harus memperhatikan:

31.5.1. Pengamanan informasi yang digunakan dalam proses pengembangan sistem informasi.

31.5.2. Pengendalian akses ke lingkungan pengembangan.

31.5.3. Pemisahan lingkungan pengembangan dengan lingkungan pengujian dan operasional.

31.5.4. Backup data dan software yang digunakan di lingkungan pengembangan.

31.5.5. Pemisahan secara fisik, logical, maupun pengguna antarlingkungan pengembangan, pengujian, dan operasional.

31.5.6. Pengendalian perpindahan informasi antarlingkungan pengembangan, pengujian, dan operasional.

## 32. MANAJEMEN PERUBAHAN

32.1. Seluruh perubahan dalam infrastruktur teknologi informasi dan komunikasi dan sistem aplikasi harus dikelola dan dikendalikan untuk menghindari terjadinya kegagalan dalam sistem informasi.

32.2. Pengendalian perubahan diterapkan pada infrastruktur dan Sistem harus mengacu pada prosedur yang mempertimbangkan antara lain:

32.2.1. Aspek risiko yang muncul terhadap kebutuhan bisnis.

32.2.2. Dokumentasi atas log perubahan sesuai urutan waktu perubahan.

32.2.3. Perencanaan dan pengujian perubahan.

32.2.4. Tersedianya persetujuan formal untuk usulan perubahan

32.2.5. Review dan pemantauan terhadap pelaksanaan perubahan.

32.3. Seluruh sistem operasional dan aplikasi perangkat lunak harus dikelola dan dikendalikan melalui manajemen perubahan yang formal.

32.4. Berdasarkan tingkat kepentingannya, perubahan digolongkan menjadi:

32.4.1. Perubahan normal, adalah perubahan yang telah direncanakan terlebih dahulu.

32.4.2. Perubahan darurat, dibutuhkan untuk memperbaiki permasalahan pada sistem TIK untuk mengembalikan proses operasional dengan cepat dan harus mendapatkan persetujuan dari pengelola sistem TIK yang berwenang.

32.5. Manajemen perubahan perlu mencakup namun tidak terbatas pada:

32.5.1. *Assessment* dari potensi dampak, termasuk dampak dari sisi keamanan yang mungkin muncul dari perubahan.

32.5.2. Prosedur persetujuan secara formal untuk setiap perubahan.

32.5.3. Komunikasi seluruh detail dari perubahan kepada personel yang relevan.

32.5.4. Prosedur fall-back, hal ini mencakup tanggung jawab dan prosedur untuk

membatalkan dan pemulihan dari perubahan yang gagal dan kejadian yang tidak terduga sebelumnya.

32.6. Setiap perubahan yang dilakukan perlu disetujui dan didokumentasikan.

32.7. Implementasi perubahan sistem informasi harus dikendalikan melalui penerapan prosedur formal untuk pengendalian perubahan.

32.8. Hal ini bertujuan untuk mengurangi kemungkinan terjadinya kesalahan atau kerusakan pada sistem informasi organisasi.

32.9. Setiap pengembangan baru atau perubahan pada sistem yang sudah ada perlu mengikuti proses pengendalian perubahan.

32.10. Prosedur pengendalian perubahan ini perlu mencakup proses penilaian risiko, analisa terhadap dampak dari perubahan serta spesifikasi dari kontrol keamanan yang dibutuhkan.

32.11. Prosedur ini juga harus memastikan bahwa sistem keamanan dan kontrol keamanan tidak mengalami perubahan yang dapat mengganggu keamanan dari sistem.

32.12. Pengendalian perubahan perlu mempertimbangkan beberapa hal berikut:

32.12.1. Mendokumentasikan tingkat otorisasi untuk menyetujui perubahan.

32.12.2. Memastikan bahwa perubahan diajukan oleh pengguna yang berwenang.

32.12.3. Peninjauan kontrol keamanan sistem informasi untuk menjamin bahwa perubahan yang dilakukan tidak mempengaruhi kontrol tersebut.

32.12.4. Identifikasi dari semua komponen sistem informasi yang akan mengalami perubahan beserta sistem lain yang mungkin terkena pengaruh.

32.12.5. Menjamin bahwa dokumentasi sistem informasi ikut diperbaharui mengikuti perubahan pada sistem. Hal ini termasuk menyimpan dokumentasi lama yang sudah tidak berlaku.

32.12.6. Mengendalikan perubahan versi dari sistem informasi yang mengalami perubahan.

32.12.7. Memelihara audit trail untuk setiap langkah dalam proses perubahan sistem.

32.12.8. Menjamin bahwa proses implementasi perubahan dilakukan pada saat yang tepat di mana tidak mengganggu proses bisnis yang berjalan.

32.12.9. Pengujian terhadap perubahan terhadap sistem, termasuk instalasi patch dan update, perlu dilakukan pada lingkungan yang berbeda dengan lingkungan *production*.

32.13. Sistem informasi yang kritikal harus ditinjau dan diuji kembali apabila terdapat perubahan platform operasinya (sistem operasi, *middleware, database*) untuk memastikan tidak ada dampak yang dapat mengganggu operasional maupun keamanan informasi pada sistem tersebut.

32.14. 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.

32.15. Proses tersebut mencakup namun tidak terbatas pada:

32.15.1. Peninjauan pada kontrol keamanan dan integritas pada sistem informasi.

32.15.2. Mengalokasikan sumber daya, termasuk personel, waktu dan biaya, untuk menjamin peninjauan dan pengujian sistem yang disebabkan oleh perubahan pada sistem operasi.

32.15.3. Menjamin bahwa proses perubahan pada sistem operasi memberikan waktu yang cukup untuk pengujian dan peninjauan kepada aplikasi bisnis.

32.16. Modifikasi pada paket software sebaiknya tidak dilakukan atau hanya dibatasi pada perubahan yang sangat dibutuhkan. Selain itu semua perubahan harus dikendalikan dengan ketat.

32.17. Perubahan atau modifikasi perangkat lunak yang di-supply oleh Pihak Ketiga harus dibatasi. Hal berikut perlu diikuti apabila perubahan tersebut harus dipertimbangkan:

32.17.1. Risiko berubahnya proses pengendalian integritas input, proses serta output yang sudah ada dalam aplikasi.

32.17.2. Izin dari vendor aplikasi harus didapatkan.

32.17.3. Dampak bahwa dengan perubahan tersebut pihak organisasi menjadi bertanggung jawab untuk proses pemeliharaan aplikasi di masa mendatang.

32.18. 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. Setiap perubahan atau modifikasi perlu diuji dan divalidasi.

32.19. Perlindungan Data Uji

Beberapa hal berikut perlu dipertimbangkan untuk melindungi data operasional yang akan digunakan untuk kebutuhan pengujian sistem:

32.19.1. Pengendalian akses yang berlaku untuk sistem production juga diberlakukan pada sistem untuk pengujian.

32.19.2. Perlunya proses persetujuan formal untuk penyalinan (copy) dan penggunaan data operasional untuk kebutuhan pengujian sistem.

32.19.3. Setelah proses pengujian selesai, data operasional tersebut harus segera dihapus.

32.19.4. Penyalinan (*copy*) dan penggunaan data operasional perlu didokumentasikan dengan baik.

## 33. PERLINDUNGAN SISTEM INFORMASI SELAMA AUDIT

33.1. Kebutuhan audit dan aktivitas yang melibatkan pemeriksaan sistem operasional harus direncanakan dan disetujui untuk meminimalkan risiko gangguan pada proses bisnis.

33.2. Auditor sistem informasi perlu merencanakan kebutuhan audit yang melibatkan pemeriksaan sistem operasional yang meliputi:

33.2.1. Ruang lingkup dari pemeriksaan audit harus disepakati dan dikontrol.

33.2.2. Seluruh akses ke sistem informasi harus dimonitor dan dicatat dalam log untuk menghasilkan *reference trail*.

33.2.3. Pelaksana audit harus memiliki independensi dari aktivitas yang diaudit.

33.2.4. Audit requirements perlu disetujui dengan pihak manajemen yang terkait.

33.2.5. Hak akses terhadap data dan aplikasi dalam proses audit perlu dibatasi dengan akses *read only*.

33.2.6. 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.

33.2.7. Sumber daya yang dibutuhkan untuk melakukan audit harus diidentifikasi dan kemudian disediakan.

33.2.8. Proses audit test pada sistem informasi perlu dilakukan di luar jam operasional organisasi.

33.2.9. Seluruh prosedur, *requirements* dan tanggung jawab dalam proses audit sistem informasi harus didokumentasi.

# BAB VI PENUTUP

Kebijakan keamanan informasi di Lingkungan Diskominfo Kab. Kendal ini ditetapkan sebagai pedoman dalam melindungi aset informasi Diskominfo Kab. Kendal dari berbagai bentuk ancaman baik dari dalam maupun dari luar, dengan tujuan untuk menjamin kerahasiaan, keutuhan dan ketersediaan aset informasi.

Hal-hal yang bersifat teknis dan spesifik yang belum diatur dalam Kebijakan keamanan informasi ini, secara khusus akan diatur dalam buku pedoman, atau dapat dilaksanakan langsung sesuai dengan standar operasional prosedur.