



DIGITAL
TALENT
SCHOLARSHIP



PeMAHAMAN Sistem manajemen keamanan informasi berbasis sni iso/iec 27001:2013

Materi 6 – Klausul 8 Operasi



KOMINFO



#JADIJAGOANDIGITAL

Badan Penelitian dan Pengembangan Sumber Daya Manusia

Profil Pengajar



AKBAR ARYANTO

- Join BSN 2005
- Koordinator Kelompok Substansi Infrastruktur dan Keamanan Informasi PUSDATIN – BSN
- Universitas Gunadarma 1998
- University of Twente – Netherlands 2016
- Universitas Gunadarma 2021
- Asesor SMKI 27001:2013 – KAN
- Lead Auditor SMKI 27001:2013
- akbar@bsn.go.id

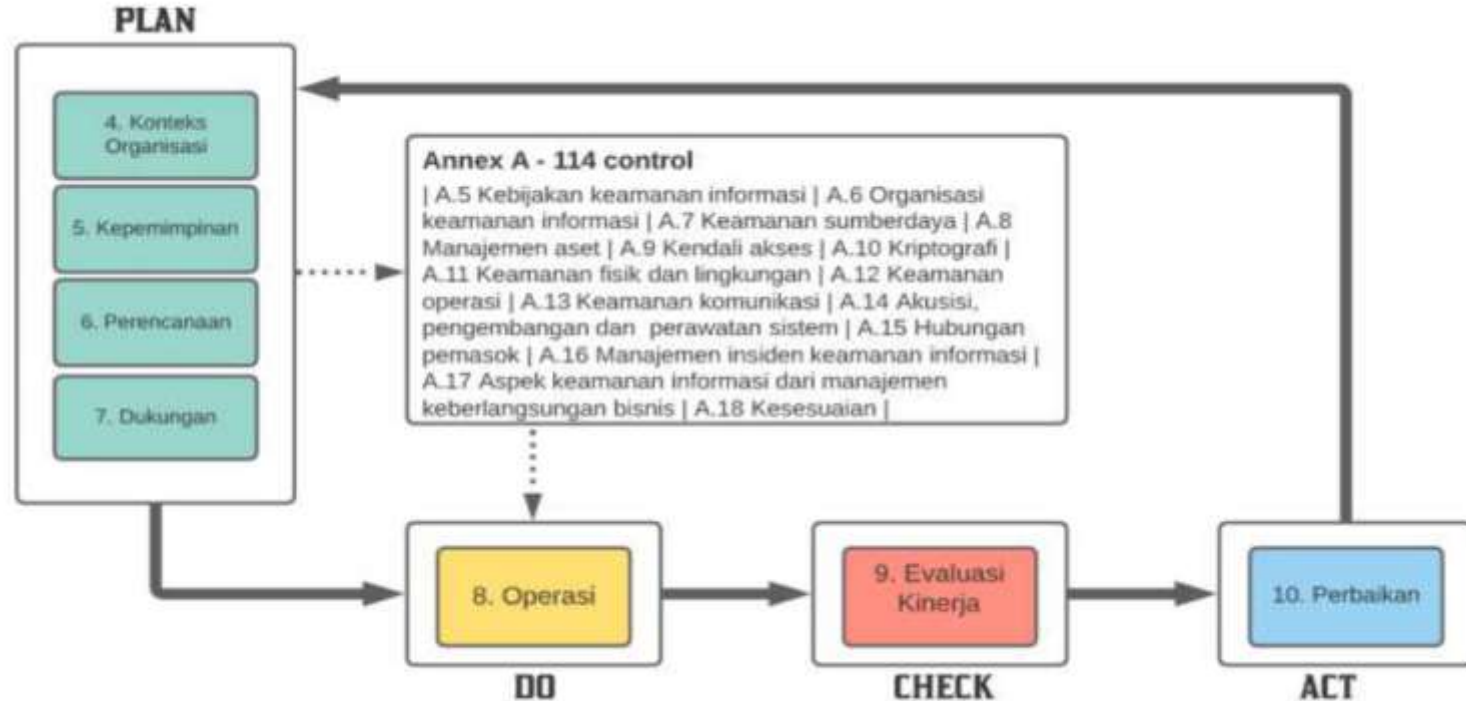


Indra Hikmawan

- S1 Sistem Informasi Universitas Gunadarma
- Pranata Komputer Ahli Pertama Pusat Data dan Sistem Informasi BSN
- Auditor & Implementer SNI ISO/IEC 27001:2013
 - Indra.hikmawan@bsn.go.id



Siklus PDCA SNI ISO/IEC 27001:2013



Klausul 8.1 Perencanaan dan Pengendalian Operasi

- Organisasi harus merencanakan, menerapkan dan mengendalikan proses yang diperlukan untuk memenuhi persyaratan keamanan informasi, dan untuk menerapkan tindakan yang ditentukan dalam 6.1. Organisasi juga harus menerapkan rencana untuk mencapai sasaran keamanan informasi yang ditentukan dalam 6.2.
- Organisasi harus menyimpan informasi terdokumentasi selama yang diperlukan untuk memiliki keyakinan bahwa proses telah dilakukan seperti yang direncanakan.
- Organisasi harus mengendalikan perubahan yang direncanakan dan mereviu konsekuensi dari perubahan yang tidak diinginkan, mengambil tindakan seperlunya untuk mengurangi efek buruk.
- Organisasi harus memastikan bahwa proses yang dialih dayakan telah ditetapkan dan dikendalikan.

A.5. Kebijakan Keamanan Informasi

A.5.1 Arahan manajemen untuk keamanan informasi

Sasaran : Untuk Memberikan arah dan dukungan manajemen untuk keamanan informasi sesuai dengan persyaratan bisnis dan regulasi dan hukum yang relevan

A.5.1.1 Kebijakan untuk keamanan informasi

Kebijakan untuk keamanan informasi harus ditetapkan, disetujui oleh manajemen, diterbitkan dan Dikomunikasikan kepada karyawan dan pihak luar yang terkait



A.5. Kebijakan Keamanan Informasi

A.5.1.2 Reviu Kebijakan keamanan informasi

Kebijakan untuk keamanan informasi harus ditinjau pada interval yang direncanakan atau jika signifikan perubahan terjadi untuk memastikan kesesuaian, kecukupan, dan keefektifannya yang berkelanjutan.

A.5. Kebijakan Keamanan Informasi

Kebijakan Sistem Manajemen Keamanan Informasi Organisasi

1. Menerapkan SNI ISO/IEC 27001:2013 sebagai sistem formal terdokumentasi untuk melindungi kerahasiaan, keutuhan dan ketersediaan informasi.
2. Organisasi menyusun objektif keamanan informasi setiap tahun dan mengukur kinerjanya setiap bulan sekali.
3. Organisasi berkomitmen untuk memenuhi semua persyaratan yang bisa diterapkan terkait keamanan informasi.
4. Organisasi berkomitmen untuk peningkatan secara berkelanjutan atas Sistem Manajemen Keamanan Informasi.

Kebijakan ini harus diketahui oleh seluruh pegawai, khususnya unit yang mengembangkan, menerapkan, memiliki dan mengelola aplikasi sistem informasi.

A.5.1.1

Penyampaian informasi kebijakan ini dilakukan melalui berbagai sarana komunikasi yang dimiliki

Kebijakan SMKI ditinjau dan dievaluasi setiap 1 tahun atau dapat dipercepat jika dipandang perlu oleh manajemen puncak

A.5.1.2

A.6. Organisasi Keamanan Informasi

A.6.1 Organisasi Internal

Tujuan: Untuk menetapkan kerangka kerja manajemen untuk memulai dan mengontrol implementasi dan operasi keamanan informasi dalam organisasi.

A.6.1.1. Peran dan tanggung jawab keamanan informasi

Semua tanggung jawab keamanan harus didefinisikan dan dialokasikan.

menetapkan dengan jelas siapa penanggung jawab SMKI agar sesuai dengan standar

menetapkan siapa yang melaporkan kinerja SMKI ke Top Manajemen?

menetapkan siapa pelaksana teknis penerapan SMKI?

A.6. Organisasi Keamanan Informasi

A.6.1.2 Pemisahan tugas

untuk menghindari kewenangan berlebihan

untuk mengurangi kemungkinan dari modifikasi yang tidak sah atau tidak sengaja atau penyalahgunaan set organisasi

untuk menghindari ketergantungan terhadap seseorang yang bisa berdampak pada organisasi



A.6. Organisasi Keamanan Informasi

A.6.1.3 Hubungan dengan pihak berwenang

Hubungan baik dengan pihak berwenang terkait harus dipelihara

Memiliki List dokumen dengan siapa organisasi bekerja sama

Siapa yang akan kita hubungi -

Bagaimana dan dalam keadaan apa kita menghubungi

GOV-CSIRT



A.6. Organisasi Keamanan Informasi

A.6.1.4 Hubungan dengan kelompok minat khusus

Hubungan baik dengan komunitas, forum, dan asosiasi professional spesialis keamanan harus dipelihara



A.6. Organisasi Keamanan Informasi

A.6.1.5 Keamanan informasi dalam manajemen proyek

Keamanan informasi harus diterapkan ke dalam manajemen proyek, tanpa memperhatikan tipe proyeknya.

Pernyataan Menjaga Kerahasiaan (*Non Disclosure Agreement*) bagi personil yang melakukan akses informasi penting/rahasia

Identifikasi risiko keamanan dalam proyek TI

Melaporkan dan menangani insiden keamanan informasi yang terjadi selama proyek berlangsung

Penutupan user id penyedia jasa/vendor setelah pekerjaan selesai

A.6. Organisasi Keamanan Informasi

A.6.2 Perangkat bergerak (mobile device) dan teleworking

A.6.2.1 Kebijakan perangkat bergerak

Kebijakan dan tindakan keamanan yang mendukung harus diadopsi untuk mengelola risiko yang terjadi akibat dan penggunaan perangkat bergerak



Memastikan OS harus updated

Memastikan memiliki antivirus

Berhati-hati ketika menggunakan WIFI public

Akses Kontrol

A.6. Organisasi Keamanan Informasi

A.6.2 Perangkat bergerak (mobile device) dan teleworking

A.6.2.1 Teleworking

Kebijakan dan tindakan keamanan yang mendukung harus diimplementasikan untuk melindungi informasi yang diakses, diproses atau disimpan ketika menjalankan teleworking



Kondisi lingkungan kerja harus aman

Berhati-hati ketika menggunakan WIFI

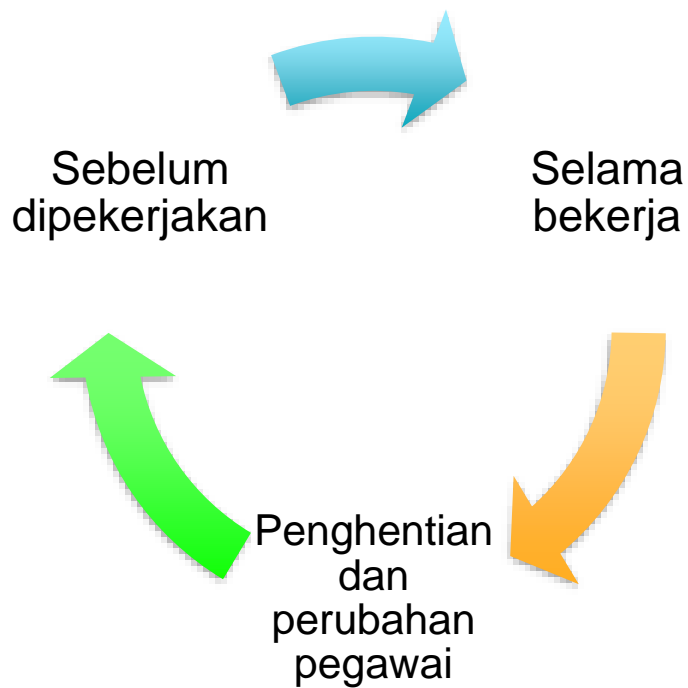
Perangkat untuk akses secara tele harus diinstall AV

Mentandatangani formulir akses teleworking

A.6.2 Perangkat bergerak (mobile device) dan teleworking

- *Aturan membawa dan menggunakan laptop/tablet/smartphone*
- *Aturan menggunakan wifi Public atau wifi yang disediakan oleh hotel/restaurant*
- *Aturan masuk ke jaringan internal*
- *Aturan masuk ke data sharing*
- *Aturan penggunaan perangkat bergerak harus mempertimbangkan:*
 - a) pendaftaran perangkat seluler;*
 - b) persyaratan untuk proteksi fisik;*
 - c) pembatasan instalasi perangkat lunak;*
 - d) persyaratan untuk versi perangkat lunak perangkat seluler dan untuk menerapkan tambalan;*
 - e) pembatasan koneksi ke layanan informasi;*
 - f) kendali akses;*
 - g) teknik kriptografi;*
 - h) perlindungan malware;*
 - i) penonaktifan jarak jauh, penghapusan atau penguncian;*
 - j) cadangan;*
 - k) penggunaan layanan web dan aplikasi web.*

A.7. Keamanan sumber daya manusia



A.7. Keamanan sumber daya manusia

A.7.1 Sebelum dipekerjakan

Sasaran : untuk memastikan bahwa karyawan dan kontraktor memahami tanggung jawab mereka an sesuai dengan peran yang ditetapkan bagi mereka

A.7.1.1 Penyaringan

Verifikasi latar belakang dari semua calon pegawai harus dilaksanakan berdasarkan hukum, regulasi dan etika terkait dan harus proporsional terhadap persyaratan bisnis, klasifikasi informasi yang akan diakses dan risiko yang dipersepsikan

Menitipkan persyaratan khusus kepada Bagian SDM terkait background khusus dan spesifikasi khusus

Memeriksa catatan kriminal jika memungkinkan



A.7. Keamanan sumber daya manusia

A.7.1 Sebelum dipekerjakan

Sasaran : untuk memastikan bahwa karyawan dan kontraktor memahami tanggung jawab mereka an sesuai dengan peran yang ditetapkan bagi mereka

A.7.1.2 Syarat dan ketentuan kepegawaian

Perjanjian tertulis dengan pegawai dan kontraktor harus menyatakan tanggung jawab keamanan informasi mereka dan organisasi

Kontrak kerja – keamanan informasi

Pernyataan Menjaga Kerahasiaan (*Non Disclosure Agreement*)



A.7. Keamanan sumber daya manusia

A.7.2 Selama bekerja

Sasaran : untuk memastikan bahwa karyawan dan kontraktor menyadari dan memenuhi tanggung jawab keamanan informasi mereka

A.7.2.1 Tanggung jawab manajemen

Manajemen harus mewajibkan semua pegawai dan kontraktor menerapkan keamanan informasi berdasarkan kebijakan dan prosedur organisasi yang sudah ditetapkan

Memastikan pegawai patuh pada Kebijakan

Memastikan pegawai paham dan memiliki kompetensi dalam penerapan SMKI

A.7. Keamanan sumber daya manusia

A.7.2 Selama bekerja

Sasaran : untuk memastikan bahwa karyawan dan kontraktor menyadari dan memenuhi tanggung jawab keamanan informasi mereka

A.7.2.2 Kepedulian, pendidikan dan pelatihan keamanan informasi

Semua pegawai organisasi dan kontraktor (jika relevan) harus menerima kepedulian, pendidikan dan pelatihan yang memadai dan pemberitahuan secara berkala mengenai kebijakan dan prosedur organisasi, sesuai dengan fungsi kerja mereka

Pegawai diberikan informasi dan pelatihan sesuai kebutuhan SMKI

Informasi bagaimana prosedur2 yang berlaku dilaksanakan

Informasi bagaimana pegawai melaporkan ketidaksesuaian



A.7. Keamanan sumber daya manusia

A.7.2 Selama bekerja

Sasaran : untuk memastikan bahwa karyawan dan kontraktor menyadari dan memenuhi tanggung jawab keamanan informasi mereka

A.7.2.3 Proses pendisiplinan

Harus ada proses pendisiplinan yang resmi dan terkomunikasikan terhadap penindakan pegawai yang melakukan pelanggaran keamanan informasi

Menitipkan aturan khusus kepada Bagian SDM terkait pelanggaran keamanan informasi

Perlu investigasi apakah pelanggaran yang disengaja / karena kecerobohan?

Sanksi bagi pegawai

Reward bagi pegawai



A.7. Keamanan sumber daya manusia

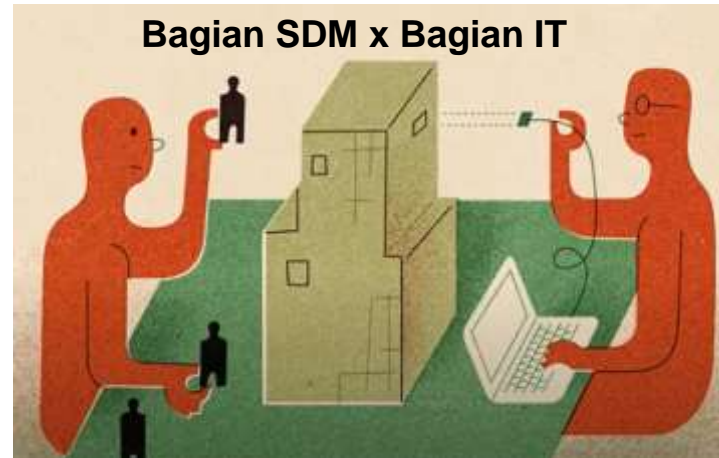
A.7.3 Penghentian dan perubahan kepegawaian

Sasaran : untuk melindungi kepentingan organisasi sebagai bagian dari proses pengubahan atau penghentian kepegawaian

A.7.3.1 Penghentian atau perubahan tanggung jawab kepegawaian

Setelah penghentian atau perubahan kepegawaian, tugas dan tanggung jawab keamanan informasi yang masih berlaku harus ditetapkan, dikomunikasikan kepada pegawai atau kontraktor dan ditegakan

Aturan harus jelas terkait hak akses (dicabut atau ditambah)



A.8. Manajemen Aset

A.8.1 Tanggung Jawab terhadap aset

Sasaran : untuk mengenali asset organisasi dan menetapkan tanggung jawab perlindungan yang sesuai

A.8.1.1 Inventaris Aset

Aset yang berhubungan dengan informasi dan fasilitas pengolahan informasi harus diidentifikasi dan inventaris aset-aset ini harus di catat dan dipelihara

Diinventarisasi / didaftarkan dan dipelihara

Data / Informasi (softcopy & hardcopy)

Software (aplikasi, O/S, tools/utility, dsb)

Hardware & Infrastruktur Jaringan

Sarana Pendukung (AC, Genset, Ruang Server, CCTV, dsb)

Aset Kritisal membutuhkan perlakuan khusus karena akan berdampak besar pada bisnis proses

A.8. Manajemen Aset

A.8.1 Tanggung Jawab terhadap aset

Sasaran : untuk mengenali asset organisasi dan menetapkan tanggung jawab perlindungan yang sesuai

A.8.1.2 Kepemilikan Aset

Aset yang dipelihara dalam inventaris harus dimiliki (ada personil yang bertanggung jawab)

Siapa yang akan bertanggung jawab terhadap asset tersebut ?

pemilik / penanggung jawabnya



A.8. Manajemen Aset

Kepemilikan Aset

Mempermudah
penelusuran



A.8. Manajemen Aset

A.8.1 Tanggung Jawab terhadap aset

A.8.1.3 Penggunaan yang dapat diterima atas aset

Aturan untuk penggunaan yang dapat diterima atas informasi dan aset yang berhubungan dengan informasi dan fasilitas pengelolaan informasi harus diidentifikasi, didokumentasi dan diimplementasikan

Ditetapkan syarat / ketentuan penggunaan aset

Penjagaan informasi di dalam aset tidak hanya fisikal



A.8. Manajemen Aset

A.8.1 Tanggung Jawab terhadap aset

A.8.1.4 Pengembalian Aset

Semua pegawai dan pengguna pihak eksternal harus mengembalikan semua asset organisasi yang dikuasainya ketika terjadi penghentian kepegawaian, kontrak atau perjanjian mereka

Ketentuan pengembalian aset

Termasuk aset informasi yan terdapat pada perangkat pribadi harus di transfer kembali ke organisasi

Catatan kepemilikan aset harus diubah



A.8. Manajemen Aset

A.8.2 Klasifikasi Informasi

Sasaran : untuk memastikan bahwa informasi mendapatkan tingkat perlindungan yang layak berdasarkan kepentingan di dalam organisasi

A.8.2.1 Klasifikasi Informasi

Informasi harus diklasifikasikan sesuai persyaratan hukum, nilai, kekritisian dan kerentanan terhadap penyingkapan atau modifikasi yang tidak sah

Prosedur klasifikasi informasi

Klasifikasi Informasi berhubungan dengan kontrol perlindungannya

A.8. Manajemen Aset

A.8.2 Klasifikasi Informasi

SANGAT RAHASIA	Data yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan menyebabkan kerugian yang sangat besar bagi organisasi
RAHASIA	Data yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan mengganggu kelancaran kegiatan organisasi atau mengganggu citra dan reputasi dari organisasi dan/atau yang menurut peraturan perundang-undangan dinyatakan rahasia.

A.8. Manajemen Aset

A.8.2 Klasifikasi Informasi

TERBATAS	Data yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan mengganggu kelancaran kegiatan organisasi tetapi tidak akan mengganggu citra dan reputasi organisasi.
PUBLIC	Data yang secara sengaja disediakan organisasi untuk dapat diketahui masyarakat umum.

A.8. Manajemen Aset

A.8.2 Klasifikasi Informasi

No	Klasifikasi	Pelabelan	Pengguna	Prasarana & Sarana
1	Biasa/ Terbuka	Tidak ada persyaratan dan prosedur khusus	Pengguna yang berasal dari eksternal dan internal yang mempunyai hak akses	Tidak memerlukan prasarana dan sarana khusus
2	Terbatas	Ada persyaratan dan prosedur dengan memberikan cap "TERBATAS" pada fisik dokumen	Dibatasi hanya untuk penentu kebijakan, pengawas internal dan eksternal serta penegak hukum	Diperlukan tempat penyimpanan yang aman
3	Rahasia	1.Ada persyaratan dan prosedur rahasia dengan memberikan cap "RAHASIA" pada fisik dokumen 2.Tidak sembarangan meletakkan arsip/ dokumen yang bersifat rahasia	Dibatasi hanya untuk penentu kebijakan, pengawas internal dan eksternal serta penegak hukum	Lokasi aman dengan akses yang terbatas
4	Sangat Rahasia	Ada persyaratan dan prosedur rahasia dengan memberikan cap "SANGAT RAHASIA" pada fisik dokumen	Dibatasi hanya untuk Penentu Kebijakan, Pengawasan, dan Penegak Hukum	1.Disimpan dalam zona yang sangat aman, dengan penelusuran jejak akses 2.Penerapan kebijakan "Meja harus bersih"

A.8. Manajemen Aset

A.8.2 Klasifikasi Informasi

No	Klasifikasi	Pelabelan	Pengguna	Prasarana & Sarana
1	Biasa/ Terbuka	Tidak ada persyaratan dan prosedur khusus	Pengguna yang berasal dari eksternal dan internal yang mempunyai hak akses	Tidak memerlukan prasarana dan sarana khusus
2	Terbatas	Ada persyaratan dan prosedur dengan memberikan cap "TERBATAS" pada fisik dokumen	Dibatasi hanya untuk penentu kebijakan, pengawas internal dan eksternal serta penegak hukum	Diperlukan tempat penyimpanan yang aman
3	Rahasia	1.Ada persyaratan dan prosedur rahasia dengan memberikan cap "RAHASIA" pada fisik dokumen 2.Tidak sembarangan meletakkan arsip/ dokumen yang bersifat rahasia	Dibatasi hanya untuk penentu kebijakan, pengawas internal dan eksternal serta penegak hukum	Lokasi aman dengan akses yang terbatas
4	Sangat Rahasia	Ada persyaratan dan prosedur rahasia dengan memberikan cap "SANGAT RAHASIA" pada fisik dokumen	Dibatasi hanya untuk Penentu Kebijakan, Pengawasan, dan Penegak Hukum	1.Disimpan dalam zona yang sangat aman, dengan penelusuran jejak akses 2.Penerapan kebijakan "Meja harus bersih"

A.8. Manajemen Aset

A.8.2 Klasifikasi Informasi

No	Klasifikasi	Pelabelan	Pengguna	Prasarana & Sarana
1	Biasa/ Terbuka	Back-up secara teratur untuk tujuan pemulihan sistem dalam rangka menjamin keaslian dokumen	Pengguna yang berasal dari eksternal dan internal yang mempunyai hak akses	Tidak memerlukan prasarana dan sarana khusus
2	Terbatas	1. Back-up secara teratur untuk tujuan pemulihan sistem dalam rangka menjamin keaslian dokumen 2. File-file elektronik (termasuk database) harus dilindungi terhadap penggunaan internal atau oleh pihak-pihak eksternal	1. Autentikasi pengguna (nama pengguna/ password atau ID digital) 2. Penggunaan untuk log in pada tingkat individual	1. Autentikasi server 2. Langkah-langkah keamanan dengan Operating System khusus atau aplikasi khusus 3. Firewall dan sistem-sistem serta prosedur-prosedur deteksi terhadap intrusi

No	Klasifikasi	Pelabelan	Pengguna	Prasarana & Sarana
3	Rahasia	1. Back-up secara teratur untuk tujuan pemulihan sistem dalam rangka menjamin keaslian dokumen 2. File-file elektronik (termasuk database) harus dilindungi terhadap penggunaan internal atau oleh pihak-pihak eksternal	1. Hanya staf yang ditunjuk oleh kementerian atau organisasi dan tingkat di atasnya yang dapat mengakses arsip tersebut 2. Autentikasi pengguna (nama pengguna/ password atau ID digital) 3. Penggunaan untuk log in pada tingkat individual	1. Langkah-langkah keamanan dengan Operating System khusus atau aplikasi khusus 2. Firewall serta sistem-sistem dan prosedur-prosedur deteksi terhadap intrusi. Firewall adalah sistem untuk melindungi komputer atau jaringan dari akses komputer lain yang tidak memiliki hak untuk mengakses komputer atau jaringan kita
4	Sangat Rahasia	1. Back-up secara teratur untuk tujuan pemulihan sistem dalam rangka menjamin keaslian dokumen 2. File-file elektronik (termasuk database) harus dilindungi terhadap penggunaan internal atau oleh pihak-pihak eksternal	1. Autentikasi pengguna (nama pengguna/ password atau ID digital) 2. Penggunaan untuk log in pada tingkat individual	1. Autentikasi server 2. Langkah-langkah keamanan dengan Operating System khusus atau aplikasi khusus 3. Firewall dan sistem-sistem dan prosedur-prosedur deteksi terhadap intrusi.

A.8. Manajemen Aset

A.8.2.2. Pelabelan informasi

Seperangkat prosedur yang tepat untuk pelabelan informasi harus dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi

Prosedur klasifikasi informasi –
menambahkan ketentuan labeling informasi



A.8. Manajemen Aset

A.8.2.3 Penanganan Aset

Prosedur penanganan aset harus dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang didapati organisasi

Prosedur harus dibuat untuk penanganan, pemrosesan, penyimpanan, dan komunikasi informasi yang konsisten dengan klasifikasinya (lihat 8.2.1).

Item berikut harus dipertimbangkan:

- a) pembatasan akses yang mendukung persyaratan perlindungan untuk setiap tingkat klasifikasi;
- b) pemeliharaan catatan resmi dari penerima aset yang berwenang;
- c) perlindungan salinan informasi sementara atau permanen ke tingkat yang konsisten dengan: perlindungan informasi asli;
- d) penyimpanan aset TI sesuai dengan spesifikasi pabrik;
- e) penandaan yang jelas dari semua salinan media untuk perhatian penerima yang berwenang.

A.8. Manajemen Aset

A.8.3 Penanganan Media

Sasaran : untuk mencegah penyingkapan, modifikasi pemindahan atau penghancuran tidak sah terhadap informasi yang disimpan di dalam media

A.8.3.1 Manajemen media yang dapat dipindahkan

Aturan-aturan perangkat penyimpanan yang dapat dipindahkan

Panduan berikut untuk pengelolaan media yang dapat dipindahkan harus dipertimbangkan:

- a) jika tidak lagi diperlukan, media harus dihapus dan harus dibuat tidak dapat dipulihkan;
- b) bila perlu dan praktis, otorisasi harus diperlukan untuk media yang dipindahkan dari organisasi dan catatan pemindahan tersebut harus disimpan untuk memelihara dan jejak audit;
- c) jika kerahasiaan atau integritas data merupakan pertimbangan penting, teknik kriptografi harus digunakan untuk melindungi data pada media yang dapat dipindahkan; (memberikan password)



A.8. Manajemen Aset



Jika tidak ada kebutuhan serius pegawai tidak diperkenankan menggunakan media yang dapat dipindahkan

Risiko data bocor

Risiko Virus

pendaftaran media yang dapat dipindahkan harus dipertimbangkan untuk membatasi peluang data kehilangan;

A.8. Manajemen Aset



Disimpan di lokasi yang aman

Hindari lokasi yang rentan terhadap panas dan lembab

Media harus dipelihara

Jika kualitas media menurun maka data harus dipindahkan ke media baru

Prosedur dan tingkat otorisasi harus didokumentasikan.

A.8. Manajemen Aset

A.8.3.2 Pembuangan media

Media harus dihancurkan dengan aman saat tidak lagi dibutuhkan dengan menggunakan prosedur baku

Prosedur harus ditetapkan

Mengatur Bagaimana, apa, kapan dan oleh siapa media di hancurkan

Dibakar, dibuang kelaut, apabila rahasia bilan memungkinkan di encrypt terlebih dahulu lalu di musnahkan

Catatan pemusnahan harus dipelihara



A.8. Manajemen Aset

A.8.3.3 Perpindahan media secara fisik

Media yang mengandung informasi harus dilindungi terhadap akses, penyalahgunaan, atau perubahan yang tidak sah selama dipindahkan.



Enkripsi Data

Penggunaan media kunci / brangkas

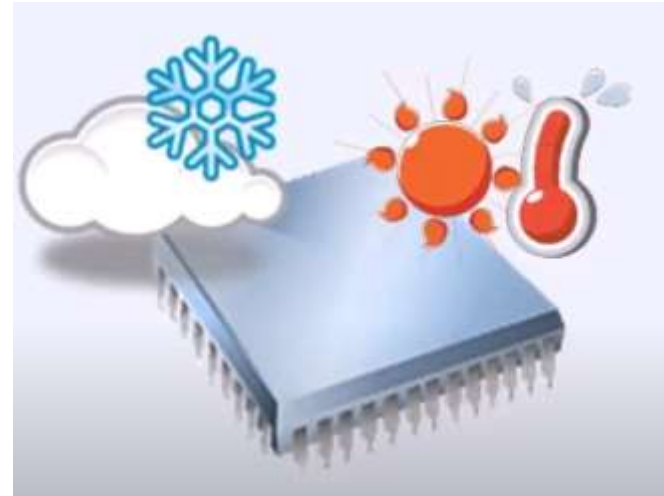
A.8. Manajemen Aset

Perpindahan media secara fisik

Media yang mengandung informasi harus dilindungi terhadap akses, penyalahgunaan, atau perubahan yang tidak sah selama dipindahkan.



Verifikasi ID Kurir



Memastikan media aman dari kondisi cuaca yang tidak bersahabat

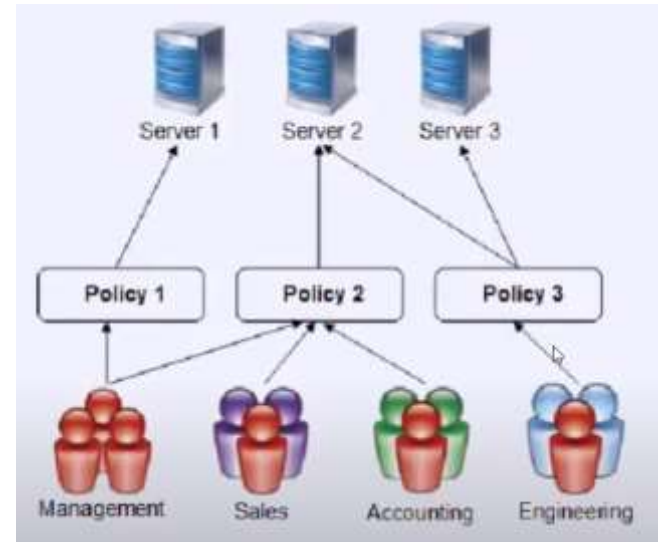
A.9. Kendali Akses

A.9.1 Persyaratan bisnis untuk kendali akses

Sasaran : untuk membatasi akses ke informasi dan fasilitas pengolahan informasi

A.9.1.1 Kebijakan kendali akses

Kebijakan kendali akses harus ditetapkan, didokumentasikan dan direviu berdasarkan dan persyaratan bisnis dan keamanan informasi

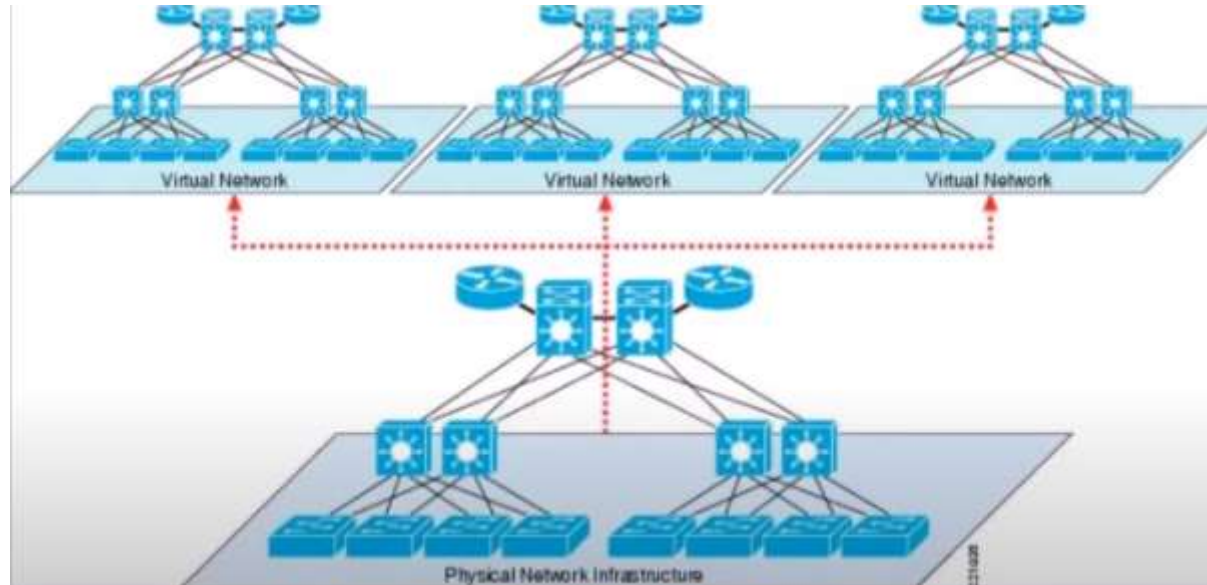


A.9. Kendali Akses

A.9.1.2 Akses ke jaringan dan layanan jaringan

Pengguna hanya akan disediakan akses ke jaringan dan layanan jaringan yang telah secara khusus diberi wewenang untuk digunakan

Kebijakan penggunaan jaringan



A.9. Kendali Akses



A.9. Kendali Akses

A.9.2 Manajemen akses pengguna

Sasaran : untuk memastikan akses pengguna yang berwenang dan untuk mencegah akses oleh pihak yang tidak berwenang ke sistem dan layanan

A.9.2.1 Registrasi dan pembatalan registrasi pengguna

Proses registrasi dan pembatalan registrasi pengguna yang resmi harus diimplementasikan untuk mengaktifkan penetapan hak akses

Prosedur manajemen hak akses

Didaftarkan dan diberikan akses yang sesuai



Ketika akses tidak lagi diperlukan maka akses harus segera dicabut

A.9. Kendali Akses

A.9.2.2 Penyediaan akses pengguna

Proses penyediaan akses pengguna yang resmi harus diimplentasikan untuk menetapkan atau mencabut hak akses untuk semua tipe pengguna ke semua sistem dan layanan



Penyediaan hak akses dilakukan sesuai kebutuhan

A.9. Kendali Akses

A.9.2 Manajemen akses pengguna

A.9.2.3 Manajemen hak akses istimewa

Pengalokasian dan penggunaan hak akses istimewa harus dibatasi dan dikendalikan.

Hak Akses istimewa diatas standar / normal
(superadmin)

Hak Akses istimewa tidak boleh digunakan untuk
aktivitas sehari-hari

Pegawai yang memiliki hak akses istimewa tidak
boleh mengambil keuntungan dari hal tersebut



A.9. Kendali Akses

A.9.2 Manajemen akses pengguna

A.9.2.5 Manajemen informasi otentikasi rahasia dari pengguna

Alokasi dari informasi otentikasi rahasia harus dikendalikan melalui proses manajemen yang resmi

Memastikan pengguna dapat menjaga informasi rahasianya



A.9. Kendali Akses

A.9.2 Manajemen akses pengguna

9.2.5 Reviu hak akses pengguna

Pemilik asset harus mereviu hak akses pengguna secara periodik

Memastikan pengguna mana yang tepat

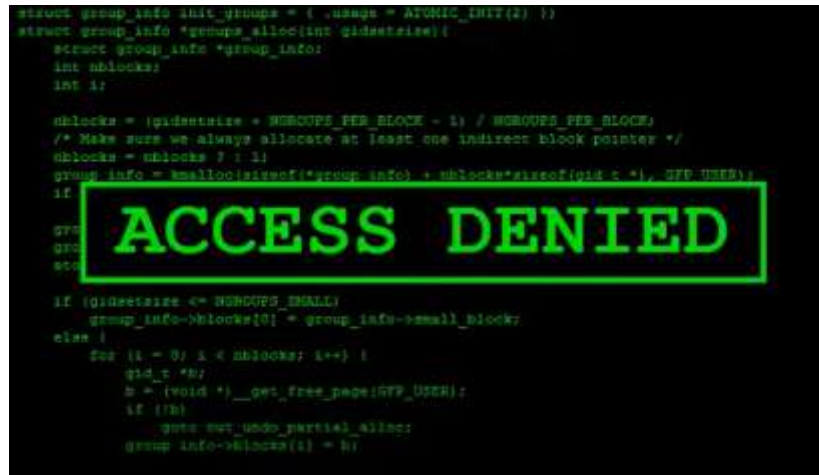


A.9. Kendali Akses

A.9.2 Manajemen akses pengguna

A.9.2.6 Penghapusan atau penyesuaian hak akses

Hak akses semua pegawai dan pengguna pihak eksternal pada informasi dan fasilitas pengolahan informasi harus dihapus sewaktu terjadi penghentian kepegawaian, kontrak atau perjanjian mereka, atau disesuaikan atas perubahan yang terjadi.



A.9. Kendali Akses

A.9.3 Tanggung jawab pengguna

Sasaran : untuk membuat pengguna bertanggung jawab dalam menjaga informasi otentikasi mereka

A.9.3.1 Penggunaan informasi otentikasi rahasia

Pengguna harus disyaratkan mengikuti praktik organisai dalam penggunaan informasi otentikasi rahasia

Aturan yang menetapkan bagaimana cara melindungi informasi

A.9. Kendali Akses

A.9.4 Kendali akses sistem dan aplikasi

Sasaran : untuk mencegah akses oleh pihak yang tidak sah ke sistem dan aplikasi

A9.4.1 Pembatasan akses informasi

Akses ke informasi dan fungsi system aplikasi harus dibatasi sesuai dengan kebijakan kendali akses

The screenshot displays the 'User Role Editor' interface. At the top, it says 'Change capabilities for user **barry** [Switch To](#)'. Below this are two checkboxes: 'Show capabilities in human readable form' and 'Show deprecated capabilities'. The main interface is divided into three columns. The first column, 'Primary Role:', has a dropdown menu set to 'Shop Manager'. Below it, 'Other Roles:' lists various roles with checkboxes: Administrator, Author, Contributor, Custom Post Widget, Customer, Editor, Plugins Manager, Settings Manager, Subscriber, Tester 888, User Manager, Vendor, WC Orders Manager, and Widgets Manager. The second column, 'Group (Total/Granted)', shows a list of groups: 'All (345/93)', 'Core (63/20)', 'General (10/4)', 'Themes (6/0)', 'Posts (13/2)', 'Pages (11/0)', 'Plugins (5/0)', 'Users (6/2)', 'Deprecated (12/10)', 'Custom Post Types (40/40)', and 'Products (17/17)'. The third column, 'Quick filter:', contains a list of capabilities with checkboxes: 'activate_plugins', 'assign_car_listing_terms', 'assign_product_terms' (checked), 'assign_shop_coupon_terms' (checked), 'assign_shop_order_terms' (checked), 'assign_shop_webhook_terms' (checked), 'copy_posts', 'create_aggregator-records', 'create_assignments', 'create_car_listings', 'create_content_blocks', 'create_courses', 'create_encyclopedia_terms', 'create_essays', 'create_events', and 'create_fmemailverifications'.

A.9. Kendali Akses

A.9.4.2 Prosedur log-on yang aman

Ketika disyaratkan oleh kebijakan pengendalian akses, akses ke system dan aplikasi harus dikendalikan oleh prosedur log-on yang aman

Lock User jika gagal lebih dari 3 kalo percobaan login

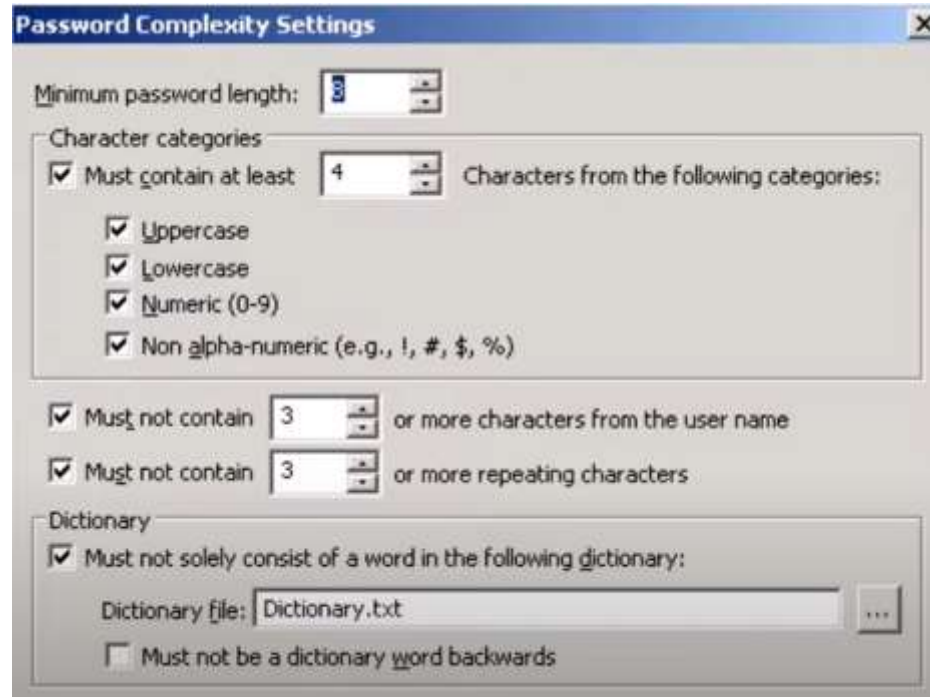
manajemen password, kompleksitas password

session time-out, pembatasan waktu koneksi

A.9. Kendali Akses

A.9.4.3 Sistem manajemen kata kunci (password)

Sistem manajemen kata kunci harus interaktif dan menjamin kualitas kata kunci



The screenshot shows a 'Password Complexity Settings' dialog box with the following options:

- Minimum password length: 8
- Character categories:
 - ☒ Must contain at least 4 Characters from the following categories:
 - ☒ Uppercase
 - ☒ Lowercase
 - ☒ Numeric (0-9)
 - ☒ Non alpha-numeric (e.g., !, #, \$, %)
- ☒ Must not contain 3 or more characters from the user name
- ☒ Must not contain 3 or more repeating characters
- Dictionary:
 - ☒ Must not solely consist of a word in the following dictionary:
 - Dictionary file: Dictionary.txt
 - ☐ Must not be a dictionary word backwards

A.9. Kendali Akses

A.9.4.4 Penggunaan program utilitas istimewa

Penggunaan program utilitas yang mungkin mampu membatalkan kendali system dan aplikasi harus dibatasi dan dikendalikan secara ketat

Risiko ketika utilitas ini digunakan, jadi perlu pengawasan / ijin tertentu



A.9. Kendali Akses

A.9.4.5 Kendali akses ke kode sumber program

Akses ke kode sumber program harus dibatasi

User yang tidak berkepentingan dapat manipulasi



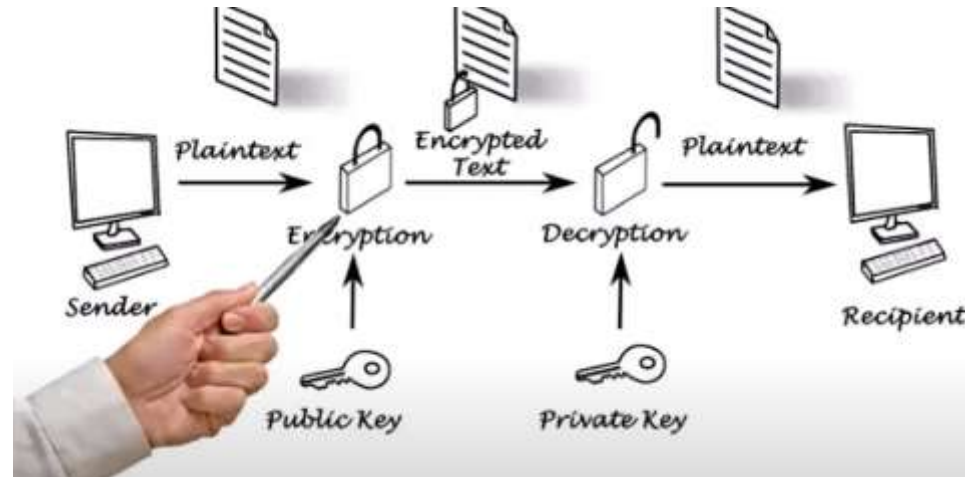
A.10. Kriptografi

A.10.1 Kendali kriptografi

Sasaran : untuk memastikan penggunaan kriptografi secara tepat dan efektif dalam melindungi kerahasiaan, keotentikkan dan/atau keutuhan

A.10.1.1. Kebijakan terhadap penggunaan kendali kriptografi

Kebijakan terhadap penggunaan kendali kriptografi untuk perlindungan informasi harus dikembangkan dan diimplementasikan



A.10. Kriptografi

A.10.1.2 Manajemen kunci

Kebijakan terhadap penggunaan, perlindungan dan masa hidup kunci kriptografi harus dikembangkan dan diimplementasikan dalam keseluruhan siklus hidupnya

Prosedur manajemen kunci
harus dibuat

Siklus hidup termasuk membuat, menyimpan,
mengarsipkan, mengambil, mendistribusikan,
menghentikan dan menghancurkan kunci.

A.11. Keamanan fisik dan lingkungan

A.11.1 Daerah aman

Sasaran : untuk mencegah akses fisik yang tidak sah, kerusakan dan interferensi terhadap informasi dan fasilitas pengolahan informasi organisasi

A.11.1.1 Batas fisik (perimeter) keamanan

Batas fisik keamanan harus ditetapkan dan digunakan untuk melindungi area yang mengandung informasi dan fasilitas pengelolaan informasi yang sensitif atau kritis

A.11. Keamanan fisik dan lingkungan

A.11.1.2 Kendali masuk fisik

Daerah aman harus dilindungi oleh kendali masuk yang sesuai untuk menjamin hanya personel berwenang saja yang diijinkan untuk mengakses



A.11. Keamanan fisik dan lingkungan

A.11.1 Daerah aman

A.11.1.3 Mengamankan kantor, ruangan dan fasilitas

Keamanan fisik untuk kantor, ruangan dan fasilitas harus dirancang dan diterapkan



Memastikan fasilitas utama harus ditempatkan untuk menghindari akses oleh publik;

Memastikan siapapun yang ada di luar ruangan atau kantor tidak bisa melihat apapun yang ada di dalam

Pengelolaan kamera intai (CCTV)

A.11. Keamanan fisik dan lingkungan

A.11.1.4 Menindungi terhadap ancaman eksternal dan lingkungan

Perlindungan fisik terhadap bencana alam, serangan jahat atau kecelakaan harus dirancang dan diterapkan

Mengupayakan Ruang Data Center
Bebas banjir

A.11.1.5 Bekerja dalam daerah aman

Prosedur untuk bekerja dalam daerah aman harus dirancang dan diterapkan



A.11. Keamanan fisik dan lingkungan

A.11.1.6 Daerah pengiriman dan bongkar muat

Titik akses seperti area bongkar muat dan titik lain yang dapat dimasuki orang yang tidak berwenang harus dikendalikan dan jika mungkin, dipisahkan dari proses fasilitas pengolahan informasi untuk mencegah akses oleh pihak yang tidak berkepentingan



A.11. Keamanan fisik dan lingkungan

A.11.2 Peralatan

Sasaran : untuk mencegah kerugian, kerusakan, pencurian atau penguasaan tanpa hak (compromise) aset dan gangguan terhadap operasi organisasi

A.11.2.1 Penempatan dan perlindungan peralatan

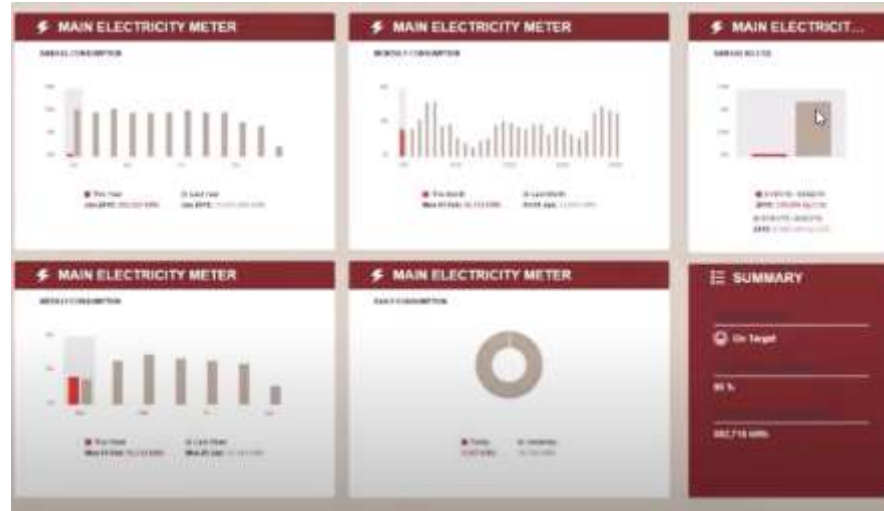
Peralatan harus ditempatkan dan dilindungi untuk mengurangi risiko dari ancaman dan bahaya lingkungan dan peluang untuk akses oleh pihak yang tidak berwenang



A.11. Keamanan fisik dan lingkungan

A.11.2..2 Utilitas pendukung

Peralatan harus dilindungi dari kegagalan catu daya dan gangguan lain yang disebabkan kegagalan utilitas pendukung



Monitoring Daya

A.11. Keamanan fisik dan lingkungan

A.11.2 Peralatan

A.11.2.3 Keamanan kabel

Kabel daya dan telekomunikasi yang memba data atau layanan informasi pendukung harus dilindungi dan pencegatan interferensi atau kerusakan

Kabel listrik dan telekomunikasi yang membawa data atau layanan informasi pendukung yang terhubung dengan perangkat dipastikan harus dilindungi,

kabel daya harus dipisahkan dari kabel komunikasi untuk mencegah interferensi;

A.11. Keamanan fisik dan lingkungan

A.11.2 Peralatan

A.11.2.4 Pemeliharaan peralatan

Peralatan harus dipelihara secara tepat untuk menjamin ketersediaan yang berkelanjutan dan integritas

A.11.2.5 Pemindahan aset

Peralatan, informasi atau perangkat lunak tidak boleh dibawa keluar lokasi tanpa izin yang berwenang

A.11. Keamanan fisik dan lingkungan

A.11.2 Peralatan

A.11.2.6 Keamanan dari peralatan dan asset di luar lokasi

Keamanan harus diterapkan untuk asset diluar kantor dengan memperhitungkan risiko yang berbeda akibat bekerja di luar lokasi organisasi

A.11.2.7 Pembuangan atau penggunaan kembali peralatan secara aman

Semua peralatan yang mengandung media penyimpanan harus diverifikasi untuk menjamin bahwa data rahasis dan perangkat lunak berlisensi apapun sudah dihapus atau ditimpa secara aman sebelumnya untuk dibuang atau dipergunakan kembali

A.11.2.8 Peralatan pengguna yang tidak diawasi

Pengguna harus menjamin bahwa peralatan yang tidak diawasi memiliki perlindungan yang layak

A.11. Keamanan fisik dan lingkungan


A.11.2 Peralatan

A.11.2.9 Kebijakan mengoskan meja dan mengosongkan layar

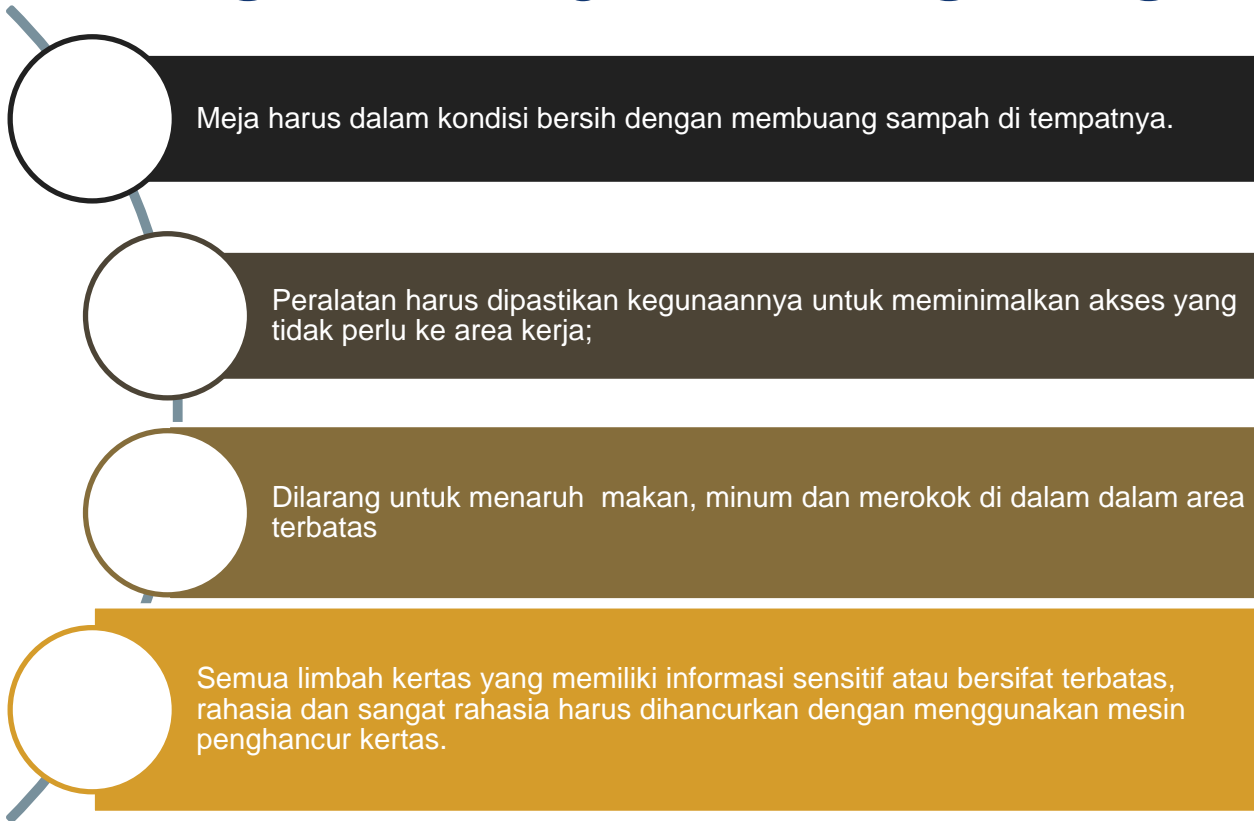
Kebijakan mengosongkan meja dari kertas dan media penyimpanan yang dapat dipindah dan kebijakan mengosongkan layar dari fasilitas pengolahan informasi harus diadopsi



Kebijakan mengoskan meja dan mengosongkan layar

- 
- 1. Komputer, laptop atau perangkat yang mengakses aplikasi dipastikan keamanannya harus dilindungi harus dikunci atau dimatikan saat meninggalkan ruangan.
 - 2. Laptop harus dimatikan dan disimpan di tempat yang aman saat meninggalkan kantor.
 - 3. Setiap berkas informasi sensitif atau bersifat terbatas, rahasia dan sangat rahasia harus dikunci didalam laci saat meninggalkan ruangan.
 - 4. Kunci yang digunakan untuk akses ke informasi sensitif atau bersifat terbatas, rahasia dan sangat rahasia tidak boleh dibiarkan tanpa pengawasan.
 - 5. Segala jenis kata sandi tidak boleh ditulis di area yang dapat diakses dengan mudah.

Kebijakan mengoskan meja dan mengosongkan layar



A.12. Keamanan Operasi

A.12.1 Prosedur dan tanggung jawab operasional

Sasaran : untuk menjamin operasi fasilitas pengolahan informasi benar dan aman

Prosedur operasional yang didokumentasikan

Prosedur operasional harus didokumentasikan dan tersedia untuk semua pengguna yang membutuhkan



A.12. Keamanan Operasi

Manajemen perubahan

Perubahan terhadap organisasi, proses bisnis, fasilitas pengolahan informasi dan system yang mempengaruhi keamanan informasi harus dikendalikan



Perubahan terkendali

Teknologi baru

Perubahan tidak terkendali

Lingkungan / Kondisi Negara

A.12. Keamanan Operasi

Manajemen kapasitas

Penggunaan sumber daya harus diawasi, diatus dan dibuat proyeksi atas kebutuhan kapasitas di masa datang untuk memastikan performa system yang dibutuhkan



Memastikan sumber daya cukup

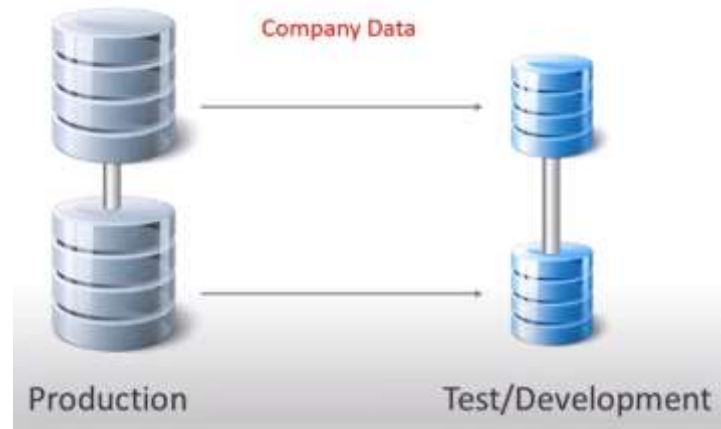
Pemantauan Storage, Bandwidth

A.12. Keamanan Operasi

A.12.1 Prosedur dan tanggung jawab operasional

Pemisahan lingkungan pengembangan, pengujian dan operasional

Lingkungan pengembangan, pengujian dan operasional harus dipisahkan untuk mengurangi risiko akses atau perubahan tidak sah pada lingkungan operasional



A.12. Keamanan Operasi

A.12.2 Perlindungan dari malware

Sasaran : untuk memastikan informasi dan fasilitas pengolahan informasi terlindungi dari malware

Kendali terhadap malware

Kendali deteksi, pencegahan dan pemulihan untuk melindungi terhadap malware harus diimplementasikan, digabungkan dengan kepedulian pengguna yang sesuai



Menggunakan end point protection

Menggunakan perlindungan perangkat security network

A.12. Keamanan Operasi

A.12.3 Cadangan (Backup)

Sasaran : untuk melindungi dari kehilangan data

Cadangan informasi

Salinan cadangan informasi, perangkat lunak dan image system harus diambil dan diuji secara berkala sesuai dengan kebijakan cadangan yang disetujui



A.12. Keamanan Operasi

A.12.4 Pencatatan (logging) dan pemantauan

Sasaran : untuk mencatat peristiwa dan menghasilkan barang bukti

Pencatatan kejadian (event logging)

Catatan kejadian yang merekam aktivitas pengguna, pengecualian(exception), kegagalan dan kejadian keamanan informasi harus diciptakan, disimpan dan direviu secara berkala

Menggunakan manajemen log terpusat

Perlindungan terhadap informasi log

Fasilitas untuk mencatat log dan informasi log harus dilindungi terhadap pemalsuan dan akses yang tidak berwenang

Otomatis backup log

Masa Retensi Log

A.12. Keamanan Operasi

A.12.4 Pencatatan (logging) dan pemantauan

Log administrator dan operator

Aktivitas administrator system dan operator system harus dicatat dan catatan tersebut dilindungi dan direviu secara berkala

Admin memiliki hak akses istimewa

Otomatisasi log

Sinkronisasi waktu

Waktu dari semua system pengolahan informasi yang terkait dalam organisasi atau wilayah keamanan harus disinkronisasikan ke sumber waktu acuan tunggal

Tujuan Investigasi

A.12. Keamanan Operasi

A.12.5 Kendali perangkat lunak operasional

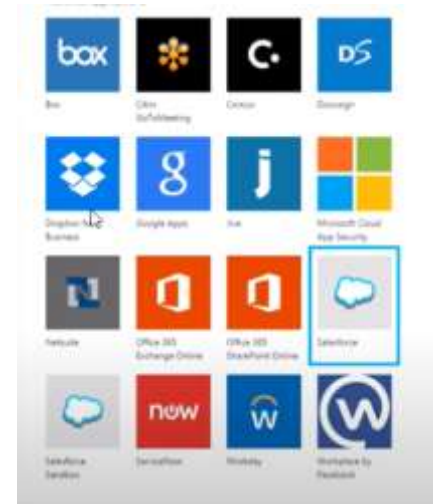
Sasaran : untuk memastikan integritas system operasional

Instalasi perangkat lunak pada system operasional

Prosedur harus diimplementasikan untuk mengendalikan instalasi perangkat lunak pada system operasional

Memastikan OS
yang digunakan –
Pro / home

Memastikan
prosedur
updating OS



A.12. Keamanan Operasi

A.12.6 Manajemen kerentanan teknis

Sasaran : untuk mencegah eksploitasi kerentanan teknis

Manajemen kerentanan teknis

Informasi mengenai kerentanan teknis system informasi yang digunakan harus diperoleh tepat waktu, keterpaparan(exposure) organisasi terhadap kerentanan tersebut dievaluasi dan tindakan yang tepat diambil untuk mengatasi risiko terkait

Aturan2 terhadap perangkat.

Mencatat versioning OS,

Win 11? Apakah cocok dengan aplikasi sebelumnya



A.12. Keamanan Operasi

Pembatasan terhadap instalasi perangkat lunak

Aturan yang mengatur instalasi perangkat lunak oleh pengguna harus ditetapkan dan diimplementasikan

Pembatasan terhadap instalasi software

Instalasi software dilakukan oleh admin



A.12. Keamanan Operasi

A.12.7 Pertimbangan audit sistem informasi

Sasaran : untuk meminimalkan dampak dari aktifitas audit system operasional

Kendali audit system informasi

Persyaratan dan aktifitas audit yang melibatkan verifikasi system operasional harus direncanakan secara hati-hati dan disepakati untuk memperkecil gangguan ke proses bisnis

Apabila kegiatan audit akan mengganggu operasional maka audit dilaksanakan di luar jam kerja

A.13. Keamanan Komunikasi

A.13.1 Manajemen keamanan jaringan

Sasaran : untuk menjamin perlindungan informasi dalam jaringan dan fasilitas pendukung pengolahan informasi

Kendali Jaringan

Jaringan harus dikelola dan dikendalikan untuk melindungi informasi dalam system dan aplikasi

Mekanisme pemantauan jaringan



A.13. Keamanan Komunikasi

Keamanan layanan jaringan

Mekanisme keamanan, tingkat layanan dan persyaratan manajemen dari semua layanan jaringan harus diidentifikasi dan dimasukkan dalam perjanjian layanan jaringan yang dapat dikerjakan sendiri atau dialihdayakan

Layanan Jaringan Internet

Layanan Jaringan Wired dan Wireless

Service level agreement

Layanan Jaringan Virtual Private Network

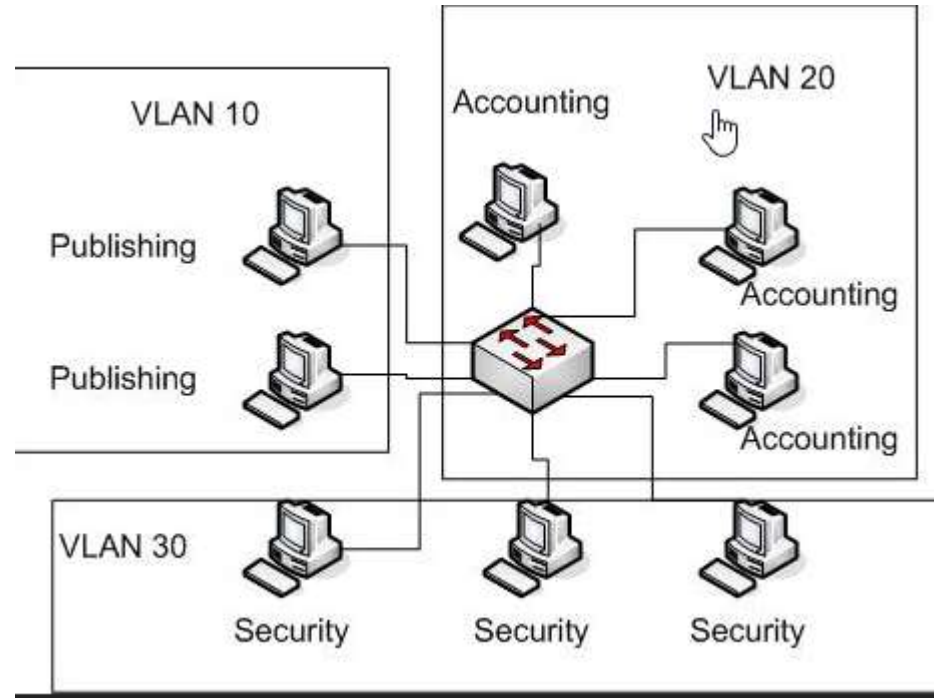
Pemisahan dalam jaringan

Kelompok layanan informasi, pengguna dan system informasi harus dipisahkan pada jaringan

A.13. Keamanan Komunikasi

Pemisahan dalam jaringan

Kelompok layanan informasi, pengguna dan system informasi harus dipisahkan pada jaringan



A.13. Keamanan Komunikasi

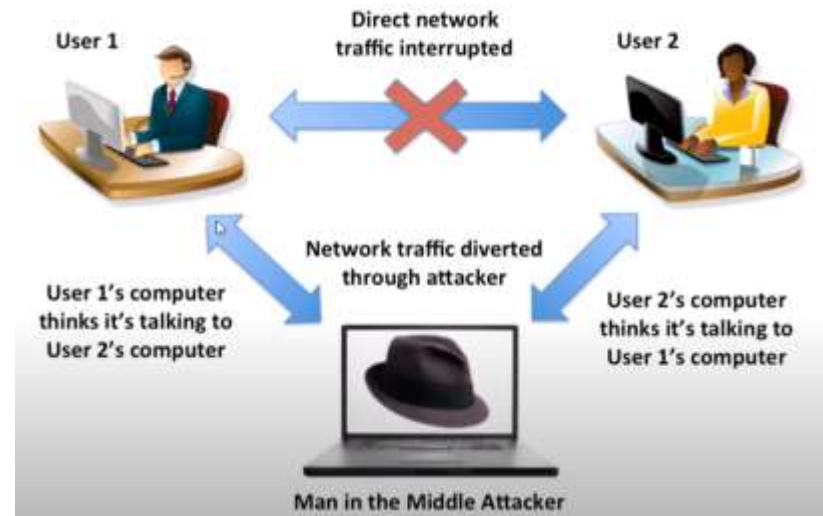
A.13.2 Perpindahan informasi

Sasaran : untuk memelihara keamanan informasi yang dipindahkan dalam suatu organisasi ataupun dengan pihak luar

Prosedur dan kebijakan perpindahan informasi

Kebijakan prosedur dan kendali perpindahan yang resmi harus ada untuk melindungi perpindahan informasi melalui penggunaan semua jenis fasilitas komunikasi

Menetapkan kebijakan perpindahan informasi



A.13. Keamanan Komunikasi

Perjanjian perpindahan informasi

Perjanjian harus mengatur perpindahan informasi bisnis yang aman Antara organisasi dan pihak eksternal

Perpindahan informasi secara elektronik

Harus dapat dilacak dan tidak dapat disangkal

Perpindahan informasi secara fisik

A.13. Keamanan Komunikasi

A.13.2 Perpindahan informasi

Pesan Elektronik

Informasi yang terdapat dalam pesan elektronik harus dilindungi dengan tepat

Memeriksa Sender

Menggunakan
Enkripsi Email



A.13. Keamanan Komunikasi

A.13.2 Perpindahan informasi

Perjanjian kerahasiaan atau menjaga rahasia

Persyaratan untuk perjanjian kerahasiaan atau menjaga rahasia mencerminkan kebutuhan organisasi untuk perlindungan informasi harus diidentifikasi, direviu secara teratur dan didokumentasikan



A.14. Akusisi, pengembangan dan perawatan sistem

A.14.1 Persyaratan keamanan sistem informasi

Sasaran : untuk memastikan bahwa keamanan informasi merupakan sebuah bagian integral dari system informasi di keseluruhan daur hidup, hal ini juga termasuk persyaratan untuk system informasi yang menyediakan layanan melalui jaringan publik

Analisis dan spesifikasi persyaratan keamanan informasi

Persyaratan yang terkait keamanan informasi harus termasuk dalam persyaratan untuk system informasi baru atau pengembangan system informasi yang ada

Harus memenuhi persyaratan keamanan informasi - environtment

Pengamanan layanan aplikasi pada jaringan publik

Informasi yang terdapat dalam layanan aplikasi yang melewati jaringan public harus dilindungi dari aktivitas yang bersifat menipu, perselisihan kontrak, dan pembukaan rahasia dan modifikasi secara tidak sah

Menggunakan secure log on - password

Menggunakan SSL

A.14. Akusisi, pengembangan dan perawatan sistem

A.14.1 Persyaratan keamanan sistem informasi

Perlindungan transaksi layanan aplikasi

Informasi yang terdapat di dalam transaksi layanan aplikasi harus dilindungi untuk mencegah transmisi yang tidak lengkap, pemilihan jalur yang salah (miss routing) pengubahan pesan yang tidak sah, pembukaan rahasia yang tidak sah, duplikasi atau balasan pesan yang tidak sah

Memastikan tidak ada kesalahan data

A.14. Akusisi, pengembangan dan perawatan sistem

A.14.2 Keamanan dalam proses pengembangan dan dukungan

Sasaran : untuk memastikan bahwa keamanan informasi dirancang dan diterapkan dalam daur hidup pengembangan system informasi

Kebijakan pengembangan yang aman

Aturan untuk pengembangan perangkat lunak dan system harus ditetapkan dan diterapkan untuk pengembangan dalam organisasi

Versioning setiap berapa tahun sekali?

Prosedur kendali perubahan sistem

Perubahan terhadap system dalam daur pengembangan harus dikendalikan dengan penggunaan prosedur kendali perubahan yang baku

A.14. Akusisi, pengembangan dan perawatan sistem

A.14.2 Keamanan dalam proses pengembangan dan dukungan

Reviu teknis aplikasi setelah perubahan platform operasi

Ketika platform operasi diubah, aplikasi kritis bisnis harus direviu dan diuji untuk memastikan tidak adanya dampak yang merugikan pada operasi atau keamanan organisasi

Peninjauan perubahan

Pembatasan dalam pengubahan paket perangkat lunak

Modifikasi pada paket perangkat lunak harus dicegah dibatasi untuk perubahan yang diperlukan dan semua perubahan harus dikendalikan dengan ketat

Memastikan tidak mengganggu yang production

A.14. Akusisi, pengembangan dan perawatan sistem

A.14.2 Keamanan dalam proses pengembangan dan dukungan

Prinsip rekayasa system yang aman

Prinsip untuk rekayasa system yang aman harus ditetapkan, didokumentasikan, dipertahankan dan diterapkan ke setiap upaya implementasi system informasi

Lingkungan pengembangan yang aman

Organisasi harus membangun dan melindungi secara memadai lingkungan pengembangan yang aman untuk upaya pengembangan dan integrasi system yang mencakup seluruh daur hidup pengembangan sistem

Ujicoba dipastikan aman

A.14. Akusisi, pengembangan dan perawatan sistem

A.14.2 Keamanan dalam proses pengembangan dan dukungan

Pengembangan oleh alihdaya

Organisasi harus mengawasi dan memantau aktivitas pengembangan system yang dialihdayakan

Kontrak

Pengujian Keamanan Sistem

Pengujian fungsi keamanan harus dilakukan selama pengembangan

Penetration Test

Pengujian penerimaan sistem

Program pengujian penerimaan dan kriteria terkait harus ditetapkan untuk system informasi baru, peningkatan dan versi baru

UAT

A.14. Akusisi, pengembangan dan perawatan sistem

A.14.3 Data Uji

Sasaran : untuk memastikan perlindungan terhadap data yang digunakan untuk pengujian

Proteksi data uji

Data uji harus dipilih dengan hati-hati, dilindungi dan dikendalikan

Data Uji yang digunakan data dummy

A.15. Hubungan Pemasok

A.15.1 Keamanan Informasi dalam hubungan pemasok

Sasaran : untuk memastikan perlindungan dari asset organisasi yang dapat diakses oleh pemasok

Kebijakan keamanan informasi untuk hubungan pemasok

Persyaratan keamanan informasi untuk mitigasi risiko yang berkaitan dengan akses pemasok untuk asset organisasi harus disetujui dengan pemasok dan didokumentasikan

Memasukan klausul keamanan dalam perjanjian pemasok

Semua persyaratan keamanan informasi yang relevan harus ditetapkan dan disetujui dengan setiap pemasok yang dapat mengakses, memproses, menyimpan, berkomunikasi atau menyediakan komponen infrastruktur TI untuk informasi organisasi

Organisasi berhak mengaudit kepada pihak pemasok


Pemenuhan SLA

A.15. Hubungan Pemasok

A.15.1 Keamanan Informasi dalam hubungan pemasok

Rantai pasok teknologi informasi dan dokumentasi

Perjanjian dengan pemasok harus termasuk persyaratan untuk mengatasi risiko keamanan informasi terkait rantai pasok layanan dan prosuk teknologi informasi dan komunikasi



Komunikasi

A.15. Hubungan Pemasok

A.15.2 Manajemen penyampaian layanan pemasok

Sasaran : untuk menjaga tingkat yang disetujui dari keamanan informasi dan penyampaian layanan dijalankan sesuai dengan yang terdapat dalam perjanjian pemasok

Pemantauan dan reviu layanan pemasok

Organisasi harus secara teratur memantau, mereviu dan mengaudit

Mengelola perubahan layanan pemasok

Perubahan ketentuan layanan oleh pemasok, termasuk mempertahankan dan meningkatkan kebijakan, prosedur dan kendali keamanan informasi yang ada harus dikelola dengan memperhitungkan tingkat kekritisn informasi system dan proses bisnis yang terlibat dan asesmen ulang terhadap risiko

Apabila ada perubahan dari layanan juga bias diatur . SLA turun atau naik..

A.16. Manajemen Insiden Keamanan Informasi

A.16.1 Manajemen insiden keamanan informasi dan perbaikan

Sasaran : untuk memastikan pendekatan konsisten dan efektif untuk manajemen insiden keamanan informasi, termasuk komunikasi tentang kejadian dan kelemahan keamanan

Tanggung Jawab dan Prosedur

Tanggung jawab dan prosedur manajemen harus ditetapkan untuk memastikan tanggapan yang cepat, efektif dan tepat untuk insiden keamanan informasi



Organisasi harus memastikan: adanya **struktur manajemen / tim** yang beranggotakan **personel yang memiliki kemampuan / kompetensi** dalam menangani sebuah insiden dan pengelolaan keamanan informasinya.

A.16. Manajemen Insiden Keamanan Informasi

A.16.1 Manajemen insiden keamanan informasi dan perbaikan

Sasaran : untuk memastikan pendekatan konsisten dan efektif untuk manajemen insiden keamanan informasi, termasuk komunikasi tentang kejadian dan kelemahan keamanan

Pelaporan kejadian keamanan informasi

Kejadian keamanan informasi harus dilaporkan melalui saluran manajemen yang sesuai secepat mungkin

Prosedur Penanganan Insiden Keamanan Informasi

A.16. Manajemen Insiden Keamanan Informasi

A.16.1 Manajemen insiden keamanan informasi dan perbaikan

Pelaporan kelemahan keamanan informasi

Karyawan dan kontraktor yang menggunakan system informasi dan layanan organisasi harus mencatat dan melaporkan kelemahan keamanan informasi yang diamati dan dicurigai dalam system dan layanan

Asesmen dan keputusan pada kejadian keamanan informasi

Kejadian keamanan informasi harus dinilai dan harus diputuskan jika akan diklasifikasikan sebagai insiden keamanan informasi

Tanggapan terhadap insiden keamanan informasi

Insiden Keamanan Informasi harus ditanggapi sesuai dengan prosedur yang telah didokumentasikan

A.16. Manajemen Insiden Keamanan Informasi

A.16.1 Manajemen insiden keamanan informasi dan perbaikan

Pembelajaran dari insiden keamanan informasi

Pengetahuan yang diperoleh dari menganalisis dan mengatasi insiden keamanan informasi harus digunakan untuk mengurangi kemungkinan insiden atau dampak insiden di masa mendatang

Pengumpulan Bukti

Organisasi harus mendefinisikan dan menetapkan prosedur untuk mengidentifikasi, mengumpulkan informasi yang dapat berguna sebagai bukti

A.17. Aspek keamanan informasi dari manajemen keberlangsungan bisnis

A.17.1 Keberlangsungan keamanan informasi

Sasaran : Keberlangsungan keamanan informasi harus ditanamkan dalam system manajemen keberlangsungan bisnis organisasi

Perencanaan keberlangsungan keamanan informasi

Organisasi harus menentukan persyaratannya untuk keamanan informasi dan keberlangsungan manajemen keamanan informasi dalam situasi yang merugikan

Contoh : selama krisis atau bencana

Mengimplementasikan keberlangsungan keamanan informasi

Organisasi harus menetapkan, mendokumentasikan, menerapkan dan menjaga proses, prosedur dan kendali yang memastikan tingkat yang dibutuhkan dalam keberlangsungan keamanan informasi selama situasi yang merugikan

Organisasi harus memastikan: adanya **struktur manajemen / tim** yang beranggotakan **personel yang memiliki kemampuan / kompetensi** dalam menangani sebuah insiden dan pengelolaan kemananan informasinya. Serta memiliki **prosedur** untuk pengelolaan insiden dan situasi yang merugikan

A.17. Aspek keamanan informasi dari manajemen keberlangsungan bisnis

A.17.1 Keberlangsungan keamanan informasi

Memeriksa, mereviu dan mengevaluasi keberlangsungan keamanan informasi

Organisasi harus memeriksa kendali keberlangsungan keamanan informasi yang ditetapkan dan diimplementasikan secara berkala dan memastikan bahwa kendali tersebut valid dan efektif selama situasi yang merugikan

Drill Test

A.17. Aspek keamanan informasi dari manajemen keberlangsungan bisnis

A.17.2 Redudansi

Sasaran : Untuk memastikan ketersediaan fasilitas pengolahan informasi

Ketersediaan fasilitas pengolahan informasi

Fasilitas pengolahan informasi harus diimplementasikan dengan redundansi yang cukup untuk memenuhi persyaratan ketersediaan.

SLA dan dilakukan drill test

A.18. Kesesuaian

A.18.1 Kesesuaian dengan persyaratan hukum dan kontraktual

Sasaran : Untuk menghindari pelanggaran hukum, undang-undang, peraturan atau kewajiban kontraktual yang terkait dengan keamanan informasi dan persyaratan keamanan lainnya.

Identifikasi persyaratan perundang-undangan dan kontraktual yang berlaku

Semua persyaratan undang-undang, peraturan, kontraktual yang relevan, dan pendekatan organisasi untuk memenuhi persyaratan ini, harus diidentifikasi secara eksplisit, didokumentasikan dan dijaga tetap mutakhir untuk setiap sistem informasi dan organisasi.

Hak kekayaan intelektual

Prosedur yang sesuai harus diimplementasikan untuk memastikan kesesuaian dengan persyaratan hukum dan perundang-undangan serta kontraktual yang terkait dengan hak atas kekayaan intelektual dan penggunaan produk perangkat lunak proprietary.

Penggunaan Software legal / berlisensi.
Penggunaan Audio/Video yang legal

A.18. Kesesuaian

A.18.1 Kesesuaian dengan persyaratan hukum dan kontraktual

Perlindungan rekaman

Rekaman harus dilindungi dari kehilangan, kerusakan, pemalsuan, akses tidak sah dan rilis tidak sah, sesuai dengan persyaratan peraturan perundangan, kontraktual dan bisnis

1. Klasifikasi informasi dengan penanganannya.
2. Masa retensi dokumen
3. Penghapusan informasi

A.18. Kesesuaian

A.18.1 Kesesuaian dengan persyaratan hukum dan kontraktual

Privasi dan perlindungan atas informasi pribadi yang dapat diidentifikasi

Privasi dan perlindungan informasi pribadi yang dapat diidentifikasi harus dipastikan sebagaimana disyaratkan dalam peraturan perundangan yang relevan.

1. GDPR bila ada
2. UU 14/2008 Keterbukaan Informasi Publik
3. UU11/2008 Informasi dan Transaksi Elektronik (ITE) UU19/2016 Perubahan UU ITE Perkominformasi 20/2016 Perlindungan data pribadi dalam Sistem Elektronik

A.18. Kesesuaian

A.18.1 Kesesuaian dengan persyaratan hukum dan kontraktual

Peraturan kendali kriptografi

kendali kriptografi harus sesuai dengan semua peraturan perundangan dan perjanjian yang relevan.

A.18. Kesesuaian

A.18.2 Reviu keamanan informasi

Sasaran : Untuk memastikan bahwa keamanan informasi diimplementasikan dan dioperasikan sesuai dengan kebijakan dan prosedur organisasi.

Reviu independen terhadap keamanan informasi

Pendekatan organisasi untuk mengelola keamanan informasi dan implementasinya (contoh: sasaran kendali, kendali, kebijakan, proses dan prosedur untuk keamanan informasi) harus direviu berkala secara independen atau ketika terjadi perubahan signifikan.

Kesesuaian dengan kebijakan dan standar keamanan

Manajer harus secara teratur mereviu kesesuaian prosedur dan pemrosesan informasi dalam area tanggung jawab mereka dengan kebijakan keamanan, standar dan persyaratan keamanan lainnya yang sesuai.

A.18. Kesesuaian

A.18.2 Reviu keamanan informasi

Reviu kesesuaian teknis

Sistem informasi harus direviu secara reguler agar tetap sesuai dengan kebijakan dan standar keamanan informasi organisasi.

- Pelaksanaan penetration test/VA harus terjadwal, terdokumentasi dan diulangi
- Pelaksanaan penetration test/VA harus dilakukan oleh personel yg kompeten dan dibawah pengawasan personel lain

Statement of Applicability (SOA)



Statement of Applicability (SOA)

Pernyataan Pemberlakuan

Versi
Tanggal

PERNYATAAN PEMBERLAKUAN / STATEMENT OF APPLICABILITY
(Nama Organisasi)
(Lingkup)

Klausul	Judul	Ya / Tidak	Justifikasi
4	Konteks Organisasi		
4.1	Konteks Organisasi untuk Keamanan Informasi		
4.1.1	Identifikasi Isu Eksternal / Internal	Ya	(Isikan alasan memenuhi/tidaknya klausul / annex tsb)
..			
..			
Annex			
A5	Information Security Policies		
A.5.1	Management Direction for Information Security		
A.5.1.1	Policies for Information Security	Ya	(Isikan alasan memenuhi/tidaknya klausul / annex tsb)
..			
..			

Klausul 8.2 Penilaian Risiko Keamanan Informasi

- Organisasi harus melakukan penilaian risiko keamanan informasi pada selang waktu terencana atau ketika perubahan signifikan diusulkan atau terjadi, dengan mempertimbangkan kriteria yang ditetapkan dalam 6.1.2 a).
- Organisasi harus menyimpan informasi terdokumentasi dari hasil penilaian risiko keamanan informasi.

Klausul 6.1.2 Penilaian risiko keamanan informasi



Klausul 8.3 Penanganan Risiko Keamanan Informasi

- Organisasi harus menerapkan rencana penanganan risiko keamanan informasi.
- Organisasi harus menyimpan informasi terdokumentasi hasil penanganan risiko keamanan informasi.

Tugas 5

1. Peserta mengidentifikasi Statement of Applicability (SOA) untuk masing-masing Instansi dengan template yang sudah disediakan
2. Peserta membuat flowchart bisnis proses:
 - a. Pengelolaan akses
 - b. Pengelolaan email
 - c. Pengelolaan asset TIK
 - d. Pengelolaan SDM
 - e. Teleworking

#Jadijagoandigital
Terima Kasih



digitalent.kominfo



DTS_kominfo



digitalent.kominfo



digital talent scholarship