LAMPIRAN

Lampiran 1
Klausal ISO 27002:2013

Klausal 5 Kebijakan Keamanan Informasi

Klausal 5 kebijakan keamanan informasi terdiri dari dua satu sub klausal yaitu Arahan manajemen manajemen untuk keamanan informasi dan

5.1 Arahan manajemen untuk keamanan informasi

Bertujuan untuk memberikan pedoman atau dukungan dalam manajemen pada keamanan informasi sesuai dengan persyaratan bisnis dan hukum yang relevan.

Tabel lampiran 1.1 Klausal arahan manajemen untuk keamanan informasi

No	Nama Klausal
5.1.1	Kebijakan untuk keamanan informasi
5.1.2	Tinjauan kebijakan untuk kemanan informasi

Klausal 6 Organisasi Keamanan Informasi

Klausal 6 terdiri dari dua sub klausal utama yaitu organisassi internal dan Perangkat seluler dan kerja jarak jauh

6.1 Organisasi internal

Bertujuan menetapkan kerangka kerja manajemen untuk pengendalian implementasi dan pengoperasian keamana informasi pada organisasi.

Tabel lampiran 1.2 Klausal organisasi internal

No	Nama Klausal
6.1.1	Peran dan tanggung jawab keamanan informasi
6.1.2	Pemisahan tugas
6.1.3	Kontak dengan pihak berwenang
6.1.4	Kontak dengan kelompok minat khusus
6.1.5	Keamanan informasi dalam manajemen proyek

6.2 Perangkat seluler dan kerja jarak jauh

Bertujuan untuk memastikan keamanan teleworking atau kerja jarak jauh dan penggunaan perangkat seluler.

Tabel lampiran 1.3 Klausal perangkat seluler dan kerja jarak jauh

No	Nama Klausal
6.2.1	Kebijakan perangkat seluler
6.2.2	Bekerja jarak jauh

Klausal 7 Keamanan Sumber Daya Manusia

Klausal 7 keamanan sumber daya manusia terdiri dari sub klausal yaitu sebelum bekerja, selama bekerja dan pemutusan hubungan kerja.

7.1 Sebelum bekerja

Bertujuan menentukan karyawan dan kontraktor mengetahui tanggung jawab mereka sesuai dengan peran yang mereka pegang.

Tabel lampiran 1.4 Klausal sebelum bekerja

No	Nama Klausal
7.1.1	Penyaringan
7.1.2	Syarat dan ketentuan kerja

7.2 Selama bekerja

Bertujuan untuk memastikan semua kontraktor dan karyawan mengetahui dan mematuhi tanggung jawab keamanan informasi.

Tabel lampiran 1. 5 Klausal selama bekerja

No	Nama Klausal
7.2.1	Tanggung jawab manajemen
7.2.2	Kesadaran, pendidikan dan pelatihan keamanan informasi
7.2.3	Proses pendisiplinan

7.3 Pemutusan hubungan kerja

Bertujuan untuk menjaga kepentingan organisasi sebagai bagian dari proses perubahan atau pemutusan hubungan kerja.

Tabel lampiran 1.6 Klausal pemutusan hubungan kerja

No	Nama Klausal
7.3.1	Pemutusan atau perubahan tanggung jawab pekerjaan

Klausal 8 Manajemen Aset

Klausal 8 manajemen aset terdiri dari tanggung jawab atas aset, Klasifikasi informasi dan penanganan media.

8.1 Tanggung jawab atas aset

Bertujuan mengidentifikasi kumpulan aset yang dimiliki organisasi dan menentukan tanggung jawab perlindungan yang sesuai.

Tabel lampiran 1.7 Klausal tanggung jawab atas aset

No	Nama Klausal
8.1.1	Inventarisasi aset
8.1.2	Kepemilikan aset
8.1.3	Penggunaan aset yang dapat dipelihara
8.1.4	Pengembalian aset

8.2 Klasifikasi informasi

Bertujuan untuk memastikan informasi mendapatkan perlindungan yang sesuai dengan tingkat kepentingan untuk organisasi.

Tabel lampiran 1.8 Klausal klasifikasi informasi

No	Nama Klausal
8.2.1	Klasifikasi informasi
8.2.2	Pelabelan informasi
8.2.3	Penanganan aset

8.3 Penanganan media

Bertujuan untuk meminimalisir pengungkapan, pengubahan, penghapusan atau penghancuran informasi yang dilakukan secara ilegal pada media yang disimpan.

Tabel lampiran 1.9 Klausal penanganan media

No	Nama Klausal
8.3.1	Manajemen media yang dapat dipindahkan
8.3.2	Pembuangan media
8.3.3	Transfer media fisik

Klausal 9 Kontrol Akses

Klausal 9 terdiri dari sub klausal persyaratan bisnis untuk kontrol akses, manajemen akses pengguna, tanggung jawab pengguna dan kontrol akses sistem dan aplikasi

9.1 Persyaratan bisnis untuk kontrol akses

Bertujuan membatasi akses kepada informasi dan infrastruktur pengelolaan informasi.

Tabel lampiran 1.10 Klausal persyaratan bisnis untuk kontrol akses

No	Nama Klausal
9.1.1	Kebijakan kontrol akses
9.1.2	Akses kejaringan dan layanan jaringan

9.2 Manajemen akses pengguna

Bertujuan untuk membatasi akses pengguna yang memiliki hak untuk mencegah akses yang tidak sah ke sistem dan layanan.

Tabel lampiran 1.11 Klausal manajemen akses pengguna

No	Nama Klausal
9.2.1	Pendaftaran dan pembatalan pendaftaran pengguna
9.2.2	Penyedian akses pengguna

No	Nama Klausal
9.2.3	Manajemen hak akses istimewa
9.2.4	Pengelolaan informasi otentikasi rahasia pengguna
9.2.5	Tinjauan hak akses pengguna
9.2.6	Penghapusan dan penyesuaian hak akses

9.3 Tanggung jawab pengguna

Bertujuan membuat pengguna memiliki tanggung jawab untuk menjaga otentikasi informasi mereka.

Tabel lampiran 1.12 Klausal tanggung jawab pengguna

No	Nama Klausal
9.3.1	Penggunaan informasi otentikasi rahasia

9.4 Kontrol akses sistem dan aplikasi

Bertujuan untuk mencegah dan meminimalisir akses tidak sah kedalam sistem dan aplikasi.

Tabel lampiran 1.13 Klausal tanggung jawab pengguna

No	Nama Klausal
9.4.1	Pembatasan akses informasi
9.4.2	Prosedur log-on yang aman
9.4.3	Sistem manajemen kata sandi
9.4.4	Penggunaan program utilitas istimewa
9.4.5	Kontrol akses ke kode sumber program

Klausal 10 Kriptografi

Klausal 10 kriptografi hanya terdiri dari 1 sub klausal yaitu kontrol kriptografi.

10.1 Kontrol kriptografi

Bertujuan untuk memastikan implementasi kriptografi yang efektif dan tepat agar kerahasian, keaslian dan integritas informasi terlindungi.

Tabel lampiran 1.14 Klausal kontrol kriptografi

No	Nama Klausal
10.1.1	Kebijakan penggunaan kontrol kriptografi
10.1.2	Manajemen kunci

Klausal 11 Keamanan Fisik dan Lingkungan

Klausal Keamanan Fisik dan Lingkungan terdiri dari sub klausal area keamanan, peralatan.

11.1 Area keamanan

Bertujuan meminimalisir akses secara fisik yang ilegal, kerusakan dan gangguan kepada informasi organisasi dan fasilitas pengelolaan informasi.

Tabel lampiran 1.15 Klausal area keamanan

No	Nama Klausal
11.1.1	Perimeter keamanan fisik
11.1.2	Kontrol entri fisik
11.1.3	Mengamankan kantor, ruangan dan fasilitas
11.1.4	Melindungi dari ancaman eksternal dan lingkungan
11.1.5	Bekerja di area aman
11.1.6	Area pengiriman dan pemuatan

11.2 Peralatan

Bertujuan untuk meminimalisir terjadinya kehilangan, kerusakan, pencurian atau kompromi aset dan gangguan pada operasi organisasi

Tabel lampiran 1.16 Klausal peralatan

No	Nama Klausal
11.2.1	Penempatan dan perlindungan alat
11.2.2	Utilitas pendukung
11.2.3	Keamanan kabel
11.2.4	Pemeliharaan peralatan
11.2.5	Penghapusan aset
11.2.6	Keamanan peralatan dan aset di luar lokasi
11.2.7	Pembuangan atau penggunaan kembali peralatan secara aman
11.2.8	Peralatan pengguna tanpa pengawasan
11.2.9	Bersihkan meja dan kebijakan layar yang jelas

Klausal 12 Operasi Keamanan

Klausal 12 operasi keamanan terdiri dari sub klausal prosedur dan tanggung jawab operasional, perlindungan malware, cadangan, pencatatan dan pemantauan, kontrol perangkat lunak operasional, manajemen kerentanan teknis dan pertimbangan audit sistem informasi.

12.1 Prosedur dan tanggung jawab operasional

Bertujuan untuk menjamin operasi yang tepat dan aman dari fasilitas pemrosesan informasi.

Tabel lampiran 1.17 Klausal prosedur dan tanggung jawab operasional

No	Nama Klausal
12.1.1	Prosedur operasi terdokumentasi
12.1.2	Manajemen perubahan
12.1.3	Manajemen kapasitas
12.1.4	Pemisahan lingkungan pengembangan, pengujian, dan operasional

12.2 Perlindungan malware

Bertujuan untuk memastikan informasi dan infrastruktur pengelolaan informasi terlindung dari malware.

Tabel lampiran 1.18 Klausal perlindungan malware

No	Nama Klausal
12.2.1	Kontrol terhadap malware

12.3 Cadangan

Bertujuan untuk menjaga dari kehilangan data.

Tabel lampiran 1.19 klausal cadangan

No	Nama Klausal
12.3.1	Cadangan informasi

12.4 Pencatatan dan pemantauan

Bertujuan untuk merekam peristiwa jika terjadi sehingga menghasilkan bukti.

Tabel lampiran 1.20 Klausal pencatatan dan pemantauan

No	Nama Klausal
12.4.1	Pencatatan peristiwa
12.4.2	Perlindungan informasi log
12.4.3	Log administrator dan operator
12.4.4	Sinkronisasi jam

12.5 Kontrol perangkat lunak operasional

Bertujuan untuk menjamin integritas sistem operasional.

Tabel lampiran 1.21 Klausal kontrol perangkat lunak operasional

No	Nama Klausal

12.5.1	Instalasi perangkat lunak pada sistem operasi

12.6 Manajemen kerentanan teknis

Bertujuan mencegah eksploitasi kerentanan teknis.

Tabel lampiran 1.22 Klausal manajemen kerentanan teknis

No	Nama Klausal
12.6.1	Manajemen kerentanan teknis
12.6.2	Pembatasan instalasi perangkat lunak

12.7 Pertimbangan audit sistem informasi

Bertujuan agar meminimalisir dampak dari aktivitas audit pada sistem operasional.

Tabel lampiran 1.23 Klausal pertimbangan audit sistem informasi

No	Nama Klausal
12.7.1	Pengendalian audit sistem informasi

Klausal 13 Keamanan Komunikasi

Klausal 13 keamanan komunikasi terdiri dari sub klausal manajemen keamanan jaringan dan transfer jaringan.

13.1 Manajemen keamanan jaringan

Bertujuan menjamin informasi dalam jaringan dan fasilitas pengelolaan informasi dan pendukungnya terlindungi.

Tabel lampiran 1.24 Klausal manajemen keamanan jaringan

No	Nama Klausal
13.1.1	Kontrol jaringan
13.1.2	Keamanan layanan jaringan
13.1.3	Segreasi dalam jaringan

13.2 Transfer jaringan

Bertujuan untuk menjaga keamanan informasi yang ditransfer dalam sebuah organisasi dengan entitas eksternal apa pun.

Tabel lampiran 1.25 Klausal transfer jaringan

No	Nama Klausal
13.2.1	Kebijakan dan prosedur transfer informasi
13.2.2	Perjanjian tentang transfer informasi
13.2.3	Pesan elektronik
13.2.4	Kerahasiaan dan perjanjian kerahasiaan

Klausal 14 Akuisi, Pengembangan dan Pemeliharaan Sistem

Klausal 14 Akuisi, Pengembangan dan Pemeliharaan Sistem terdiri dari sub klausal persyaratan keamanan sistem informasi, keamanan dalam proses Pengembangan dan dukungan dan data uji

14.1 Persyaratan keamanan sistem informasi

Bertujuan menjamin keamanan informasi adalah bagian integral dari sistem informasi di semua siklus hidup. Hal ini juga mencakup kepada sistem informasi yang menyediakan layanan dengan jaringan publik.

Tabel lampiran 1. 26 Klausal persyaratan keamanan sistem informasi

No	Nama Klausal
14.1.1	Analisis dan spesifikasi persyaratan keamanan informasi
14.1.2	Mengamankan layanan aplikasi di jaringan publik
14.1.3	Melindungi transaksi layanan aplikasi

14.2 Keamanan dalam proses pengembangan dan dukungan

Bertujuan untuk menjamin perancangan dan implementasi keamanan informasi dalam siklus hidup pengembangan sistem informasi.

Tabel lampiran 1.27 Klausal keamanan dalam proses pengembangan dan dukungan

No	Nama Klausal
14.2.1	Kebijakan pembangunan yang aman
14.2.2	Tinjauan teknis aplikasi setelah perubahan platform operasi
14.2.3	Pembatasan perubahan pada paket perangkat lunak
14.3.4	Prinsip-prinsip rekayasa sistem yang aman
14.4.4	Lingkungan pengembangan yang aman
14.4.5	Pengembangan yang dialihdayakan
14.4.6	Pengujian keamanan sistem
14.4.7	Pengujian penerimaan sistem

14.3 Data uji

Bertujuan untuk menjamin perlindungan data yang digunakan dalam pengujian.

Tabel lampiran 1.28 Klausal data uji

No	Nama Klausal
14.3.1	Perlindungan data uji

Klausal 15 Hubungan Pemasok

Klausal 15 hubungan pemasok terdiri dari sub klausal keamanan informasi dalam hubungan pemasok dan keamanan informasi dalam hubungan pemasok

15.1 Keamanan informasi dalam hubungan pemasok

Bertujuan untuk menjamin aset organisasi yang bisa diakses oleh pemasok terlindungi.

Tabel lampiran 1.29 Klausal keamanan informasi dalam hubungan pemasok

No	Nama Klausal
15.1.1	Kebijakan informasi untuk hubungan pemasok
15.1.2	Mengatasi keamanan dalam perjanjian pemasok

No	Nama Klausal
15.1.3	Rantai pemasok TI dan komunikasi

15.2 Manajemen pengiriman layanan pemasok

Bertujuan melindungi tingkat keamanan informasi dan penyampaian layanan yang telah disepakati dalam perjanjian pemasok.

Tabel lampiran 1.30 Klausal manajemen pengiriman layanan pemasok

No	Nama Klausal
15.2.1	Pemantauan dan peninjauan layanan pemasok

Klausal 16 Manajemen Insiden Keamanan Informasi

Klausal 16 manajemen insiden keamanan informasi terdiri dari sub klausal manajemen insiden dan peningkatan keamanan informasi.

16.1 Manajemen insiden dan peningkatan keamanan informasi

Bertujuan untuk menjamin pendekatan yang konsisten dan efektif untuk pemrosesan insiden keamanan informasi, termasuk komunikasi terkait peristiwa dan kelemahan keamanan.

Tabel lampiran 1.31 Klausal manajemen insiden dan peningkatan keamanan informasi

No	Nama Klausal
16.1.1	Tanggung jawab dan prosedur
16.1.2	Melaporkan peristiwa keamanan informasi
16.1.3	Melaporkan kelemahan keamanan informasi
16.1.4	Penilaian dan keputusan tentang peristiwa keamanan informasi
16.1.5	Tanggapan terhadap insiden keamanan informasi
16.1.6	Belajar dari insiden keamanan informasi
16.1.7	Pengumpulan bukti

Klausal 17 Aspek Keamanan Informasi dari Manajemen Kelangsungan Bisnis

Klausal 17 aspek keamanan informasi dari manajemen kelangsungan bisnis terdiri dari sub klausal kesinambungan keamanan informasi dan redundansi.

17.1 Kesinambungan keamanan informasi

Bertujuan kesinambungan keamanan informasi harus ditanamkan dalam sistem manajemen kelangsungan bisnis organisasi.

Tabel lampiran 1.32 Klausal kesinambungan keamanan informasi

No	Nama Klausal
17.1.1	Merencanakan kesinambungan keamanan informasi
17.1.2	Menerapkan kontinuitas keamanan informasi
17.1.3	Memverifikasi, meninjau, dan mengevaluasi kesinambungan keamanan informasi

17.2 Redundansi

Bertujuan untuk menjamin adanya fasilitas untuk pemrosesan informasi

Tabel lampiran 1.33 Klausal redundansi

No	Nama Klausal
17.2.1	Ketersediaan fasilitas pemrosesan informasi

Klausal 18 Kepatuhan

Kalusal 18 kepatuhan terdiri dari sub klausal kepatuhan terhadap persyaratan hukum dan kontrak dan tinjauan keamanan informasi.

18.1 Kepatuhan terhadap persyaratan hukum dan kontrak

Bertujuan untuk menghindari pelanggaran terkait kewajiban hukum, undang-undang, peraturan atau kontrak yang berhubungan dengan keamanan informasi dan persyaratan keamanan apa pun.

Tabel lampiran 1.34 Klausal kepatuhan terhadap persyaratan hukum dan kontrak

No	Nama Klausal
18.1.1	Identifikasi undang-undang yang berlaku dan persyaratan kontrak

No	Nama Klausal
18.1.2	Hak kekayaan intelektual
18.1.3	Perlindungan catatan
18.1.4	Privasi dan perlindungan informasi pengenal pribadi
18.1.5	Regulasi kontrol kriptografi

18.2 Tinjauan keamanan informasi

Bertujuan untuk menjamin keamanan informasi yang telah diimplementasi dan dioperasikan sesuai dengan kebijakan dan prosedur organisasi.

Tabel lampiran 1.35 Klausal tinjauan keamanan informasi

No	Nama Klausal
18.2.1	Tinjauan independen terhadap keamanan informasi
18.2.2	Kepatuhan terhadap kebijakan dan standar keamanan
18.2.3	Tinjauan kepatuhan teknis

Lampiran 2
Panduan Implementasi

Pada ISO 27002:2013, terdapat panduan implementasi yang sesuai dengan jumlah klausal yang terdapat di dalamnya. Bagian ini hanya mencantumkan panduan implementasi berdasarkan klausal yang digunakan, karena perlakuan risiko tidak melibatkan semua klausal.

Panduan implementasi klausal 7.2.2 Kesadaran, pendidikan dan pelatihan keamanan informasi

Karyawan harus dididik tentang tanggung jawab keamanan informasi mereka dan cara memenuhinya melalui program kesadaran keamanan informasi. Kebijakan keamanan informasi organisasi dan prosedur yang sesuai diikuti saat mengimplementasikan program.

Pelatihan kesadaran keamanan informasi wajib mencakup aspek umum seperti:

- Menyatakan komitmen manajemen terhadap keamanan informasi di seluruh organisasi
- Kebutuhan untuk memahami dan mematuhi aturan dan kewajiban keamanan informasi yang berlaku
- Pertanggung jawaban pribadi atas tindakan dan kelambanannya sendiri, dan tanggung jawab umum terhadap
- Pengamanan atau perlindungan informasi milik organisasi
- Prosedur keamanan informasi dasar

Pendidikan dan pelatihan keamanan informasi harus dilakukan secara berkala. Pendidikan dan pelatihan awal berlaku bagi mereka yang pindah ke posisi atau peran baru dengan persyaratan keamanan informasi yang berbeda secara substansial, tidak hanya untuk pemula dan harus dilakukan sebelum peran tersebut aktif.

Panduan implementasi klausal 7.2.3 Proses pendisiplinan

Jika seorang karyawan diduga melakukan pelanggaran keamanan informasi, prosedur pendisiplinan formal harus memastikan bahwa mereka diperlakukan secara adil. Sifat dan beratnya pelanggaran, serta dampaknya terhadap bisnis, tingkat pelatihan pelaku, undang-undang yang relevan, kontrak bisnis, dan faktor-faktor penting lainnya, semuanya harus diperhitungkan selama fase respons prosedur pendisiplinan formal.

Informasi tambahan Penting untuk berfokus pada "Mengapa" selain "apa" dan "bagaimana" saat membuat program kesadaran. Karyawan harus menyadari tujuan keamanan informasi dan potensi dampak positif dan negatif dari tindakan mereka terhadap organisasi.

Karyawan yang melanggar kebijakan, prosedur keamanan informasi organisasi, dan pelanggaran keamanan informasi lainnya juga harus dicegah melalui proses pendisiplinan. Pelanggaran yang disengaja mungkin memerlukan tindakan segera.

Panduan implementasi klausal 9.2.2 Penyediaan akses pengguna

Proses pencabutan hak akses karyawan harus mencakup:

- Memverifikasi bahwa tingkat akses yang diberikan sesuai dengan kebijakan akses
- Memastikan bahwa hak akses telah dinonaktifkan
- Mengadaptasi hak akses karyawan yang telah berganti posisi dan menghapus semua akses karyawan yang telah keluar dari organisasi
- Melakukan peninjauan hak akses setiap keryawan secara berkala

Panduan implementasi klausal 9.4.1 Pembatasan akses informasi

Pembatasan akses mesti didasari oleh kebijakan atau peraturan organisasi. Berikut hal – hal yang mesti dipertimbangkan:

- Menyediakan menu untuk mengontrol akses ke fungsi sistem
- Mengontrol data mana yang dapat diakses oleh pengguna tertentu
- Mengontrol hak akses pengguna, misalnya membaca, menulis, menghapus, dan mengeksekusi
- Menyediakan kontrol akses fisik atau logis untuk isolasi sistem sensitif, data, atau informasi

Panduan implementasi klausal 9.4.2 prosedur log-on yang aman

Teknik otentikasi harus dapat mengidentifikasi pengguna yang akan log-on. Metode autentikasi kata sandi alternatif, seperti sarana kriptografi, kartu pintar, token, atau sarana biometrik, harus digunakan di mana pun autentikasi yang kuat dan verifikasi identitas diperlukan. Masuk ke aplikasi atau sistem harus dilakukan dengan cara yang memperkecil kemungkinan orang lain untuk masuk. Oleh karena itu, untuk menghindari pemberian bantuan yang tidak perlu kepada pengguna yang tidak berwenang, prosedur masuk harus mengungkapkan informasi sesedikit mungkin tentang sistem atau aplikasi. Prosedur log-on yang baik harus:

- Sampai prosedur login berhasil diselesaikan, identifikasi sistem atau aplikasi tidak muncul.
- Memvalidasi informasi log-on hanya pada penyelesaian semua data input. Jika kondisi kesalahan muncul, sistem tidak
- Boleh menunjukkan bagian mana dari data yang benar atau salah
- Tidak menampilkan kata sandi yang dimasukkan
- Tidak mengirimkan kata sandi dalam bentuk teks yang jelas melalui jaringan

- Melindungi dari upaya masuk paksa
- Mencatat upaya yang gagal dan berhasil
- Menampilkan peringatan umum bahwa komputer hanya dapat diakses oleh pengguna yang berwenang, menghentikan sesi tidak aktif setelah jumlah ketidakaktifan yang telah ditentukan sebelumnya, khususnya di lokasi berisiko tinggi seperti area publik atau di luar manajemen keamanan organisasi atau pada perangkat seluler
- Tidak menyediakan pengguna yang tidak sah dengan pesan bantuan selama prosedur masuk
- Membatasi waktu koneksi untuk meningkatkan keamanan untuk aplikasi berisiko tinggi dan mengurangi kemungkinan akses tidak sah

Panduan implementasi klausal 9.4.3 sistem manajemen kata sandi

Sistem manajemen kata sandi harus memiliki:

- Menggunakan id dan kata sandi individu untuk menjaga akuntabilitas
- Memungkinkan pengguna untuk memilih dan memodifikasi kata sandi mereka sendiri dan menggabungkan prosedur konfirmasi untuk kemungkinan kesalahan input
- Kata sandi yang digunakan harus berkualitas
- Pengguna wajib menginput kata sandi saat log in sistem
- Kata sandi wajib diubah secara berkala
- Kata sandi tidak boleh ditampilkan di layar
- Kata sandi yang disimpan harus telah dienkripsi

Panduan implementasi klausal 11.1.4 melindungi dari ancaman eksternal dan lingkungan

Saran spesialis harus diperoleh tentang cara menghindari kerusakan akibat kebakaran, banjir, gempa bumi, ledakan, kerusuhan sipil, dan bentuk lain dari bencana alam atau bencana buatan manusia.

Panduan implementasi 11.2.1 Penempatan dan perlindungan peralatan

Berikut hal – hal yang harus dipertimbangkan dalam melindungi peralatan:

- Lokasi penyimpanan peralatan harus memiliki pemantauan akses karyawan yang masuk dan keluar.
- Alat pengolah informasi yang melindungi data sensitif harus diuji berpasangan sebelum digunakan.
- Kiriman yang terlibat dalam perlindungan khusus harus dilibatkan untuk menjamin jenis perlindungan yang digunakan.
- Tujuan dari pengendalian adalah untuk meminimalkan resiko fisik dan lingkungan, serta risiko lainnya seperti pencurian, kebakaran, bahan peledak, asap, udara (atau kegagalan suplai air), debu, getaran, efek kimia,

gangguan suplai listrik, gangguan komunikasi, radiasi elektromagnetik, dan vandalisme.

- Perlindungan hewan peliharaan harus diterapkan pada berbagai permukaan, dan filter perlindungan hewan peliharaan harus digunakan.
- Kondisi lingkungan harus dipantau, harus terdapat tindakan terdapat kondisi yang berpotensi mengganggu jalannya peralatan.
- Terdapat pedoman yang mengatur aktivitas (seperti minum, makan, merokok, dll) karyawan didekat tempat penyimpanan peralatan.
- Peralatan yang memproses informasi rahasia harus dilindungi untuk meminimalkan risiko kebocoran informasi akibat radiasi elektromagnetik.

Panduan implementasi klausal 11.2.2 utilitas pendukung

Utilitas pendukung misalnya listrik, telekomunikasi, pasokan air, gas, pembuangan limbah, ventilasi dan pendingin udara harus:

- Spesifikasi yang digunakan mesti sesuai dengan peralatan dan persyaratan hukum yang berlaku
- Pemantauan harus dilakukan secara teratur untuk memastikan peralatan tetap memenuhi kebutuhan organisasi
- Pengujian harus dilakukan secara berkala untuk memastikan fungsinya berjalan dengan sesuai kebutuhan
- Jika perlu, harus siap dalam melakukan pendeteksian malfungsi

Panduan impelementasi klausal 11.2.3 keamanan kabel

Berikut pedoman yang bisa dipertimbangkan untuk keamanan kabel:

- Saluran listrik dan telekomunikasi ke fasilitas pemrosesan informasi harus berada di bawah tanah, jika memungkinkan
- Kabel daya harus dipisahkan dari kabel komunikasi untuk mencegah interferensi
- Untuk sistem sensitif, kontrol lebih lanjut perlu mempertimbangkan
    - Akses terkontrol ke panel patch dan ruang kabel
    - Pemasangan saluran lapis baja dan kamar atau kotak terkunci pada titik inspeksi dan penghentian
    - Penggunaan pelindung elektromagnetik untuk melindungi kabel
    - Inisiasi pembersihan teknis dan inspeksi fisik untuk perangkat yang tidak sah yang terpasang kabel

Panduan implementasi klausal 11.2.4 Pemeliharaan peralatan

Berikut pedoman yang dapat dipertimbangan dalam pemeliharaan peralatan:

- Peralatan harus dipelihara sesuai dengan interval servis yang direkomendasikan

- Pemeliharaan peralatan hanya boleh dilakukan oleh karyawan resmi
- Pengendalian yang tepat harus diimplemtasikan ketika peralatan dijadwalkan untuk pemeliharaan, denganmempertimbangkan apakah pemeliharaan ini dilakukan oleh karyawan di lokasi atau diluar, Jika perlu, informasi rahasia harus dibersihkan dari peralatan terlebih dahulu
- Sebelum mengoperasikan kembali peralatan setelah pemeliharaannya, peralatan tersebut harus diperiksa untuk memastikan bahwa peralatan tersebut tidak dirusak dan tidak mengalami malfungsi

Panduan implementasi klausal 12.1.3 Manajemen kapasitas

Pentingnya bisnis harus dipertimbangkan saat menentukan persyaratan kapasitas. Pengaturan dan pemantauan sistem diperlukan untuk menjamin ketersediaan sistem dan, jika perlu, meningkatkan efisiensi sistem. Untuk segera mengidentifikasi masalah, kontrol detektif harus diterapkan. Persyaratan bisnis dan sistem baru, serta tren saat ini dan yang diantisipasi dalam kemampuan pemrosesan informasi organisasi, harus diperhitungkan saat memperkirakan kebutuhan kapasitas di masa depan.

Setiap sumber daya dengan waktu tunggu pengadaan yang lama atau biaya tinggi memerlukan perhatian khusus. Akibatnya, manajer harus mengawasi seberapa penting sumber daya sistem digunakan. Mereka harus mengidentifikasi tren penggunaan, khususnya dalam kaitannya dengan aplikasi bisnis atau alat manajemen untuk sistem informasi.

Peningkatan kapasitas atau penurunan permintaan dapat digunakan untuk menyediakan kapasitas yang memadai. Contoh mengelola kapasitas meliputi:

- Data yang tidak digunakan lagi dapat dihapus
- Dekomisioning aplikasi, sistem, database atau lingkungan
- Mengoptimalkan jadwal dan proses batch
- Mengoptimalkan kueri database dan logika sistem
- Membatasi bandwidth pada layanan yang tidak membutuhkan sumber daya besar

Panduan implementasi klausal 12.2.1 kontrol terhadap malware

Akses sistem yang tepat dan kontrol manajemen perubahan, kesadaran akan keamanan informasi, dan perangkat lunak pendeteksi dan perbaikan malware harus menjadi dasar perlindungan malware. Berikut pedoman yang dapat dipertimbangkan:

- Melarang penggunaan perangkat lunak bajakan
- Mengontrol, mencegah atau mendeteksi penggunaan perangkat lunak bajakan

- Menerapkan kontrol yang mencegah atau mendeteksi penggunaan situs web berbahaya
- Menetapkan kebijakan formal untuk melindungi terhadap risiko yang terkait dengan memperoleh file dan perangkat lunak melalui jaringan eksternal atau media lain. Jika diperlukan memberikan rekomendasi tindakan
- Menerapkan kontrol yang mencegah atau mendeteksi penggunaan situs web berbahaya
- Mengurangi kerentanan yang dapat dieksploitasi oleh malware, misalnya melalui kerentanan teknis
- Pemantauan secara rutin terhadap perangkat lunak dan konten data dari sistem yang mendukung proses bisnis. Keberadaan file yang tidak sah dan dicurigai harus segera ditindaklanjuti.
- Perangkat lunak pendeteksi dan perbaikan malware harus diinstal dan diperbarui secara berkala untuk memindai komputer dan media sebagai kontrol pencegahan,
- Menyiapkan skenario pemulihan sistem jika terjadi serangan malware

Panduan implementasi klausal 12.3.1 cadangan informasi

Persyaratan organisasi untuk mencadangkan informasi, perangkat, perangkat lunak, dan sistem harus diuraikan dalam kebijakan pencadangan. Kebijakan pencadangan mesti menentukan persyaratan penyimpanan dan perlindungan. Jika terjadi bencana atau kegagalan media, fasilitas pencadangan yang memadai harus disediakan untuk memastikan bahwa semua perangkat lunak dan informasi penting dapat dipulihkan. Beberapa hal yang harus dipertimbangkan:

- Catatan dari salinan cadangan dan restorasi yang didokumentasi harus dibuat
- Frekuensi cadangan harus disesuaikan kepentingan bisnis organisasi
- Cadangan harus disimpan pada tempat yang aman
- Informasi cadangan harus dilindungi
- Penting untuk menguji media cadangan secara teratur untuk memastikannya aman digunakan dalam keadaan darurat.
- Jika cadangan menyimpan data yang sangat sensitif maka diperlukan enkripsi

Panduan implementasi klausal 12.4.2 perlindungan informasi log

Dengan menyertakan fasilitas logging untuk memastikannya aman digunakan dalam keadaan darurat, kontrol harus bertujuan untuk mencegah perubahan tidak sah pada informasi log dan masalah operasional.

- Perubahan jenis pesang yang direkam
- File log yang diedit atau dihapus

- Memori penyimpanan log yang penuh, mengakibatkan kegagalan perekaman aktivitas log

Sebagian besar informasi dalam log sistem tidak relevan dengan data pemantauan keamanan, itulah sebabnya sering dimuat dalam jumlah besar. Pertimbangkan untuk menggunakan utilitas sistem atau alat audit yang sesuai untuk menginvestigasi dan merasionalisasi file atau secara otomatis menyalin jenis pesan yang sesuai ke dalam log kedua untuk membantu mengidentifikasi peristiwa penting untuk pemantauan keamanan informasi.

Log sistem harus dilindungi karena keberadaannya dapat menimbulkan rasa aman yang salah jika data dapat diubah atau dihapus. Log dapat dilindungi dengan menyalinnya secara real time ke sistem tanpa izin administrator sistem atau operator.

Panduan implementasi klausal 12.6.1 manajemen kerentanan teknis

Vendor perangkat lunak, nomor versi, status penerapan saat ini (seperti perangkat lunak mana yang diinstal pada sistem mana), dan individu atau individu dalam organisasi yang bertanggung jawab atas perangkat lunak adalah contoh informasi spesifik yang diperlukan untuk mendukung kerentanan teknis pengelolaan. Tindakan yang dilakukan tepat waktu harus diambil untuk mananggapi kerentanan teknis. Berikut panduan membuat manajemen kerentanan teknis:

- Peran dan tanggung jawab manajemen kerentanan teknis harus ditentukan dan ditetapkan oleh organisasi. Ini termasuk pemantauan kerentanan, penilaian risiko kerentanan, penambalan, pelacakan aset, dan tanggung jawab koordinasi yang diperlukan.
- Perangkat lunak dan sumber daya informasi terkait teknologi lainnya harus diidentifikasi. Sumber daya ini akan digunakan untuk mengidentifikasi kerentanan teknis yang relevan dan menjaga kewaspadaan terhadapnya. Sumber daya informasi ini harus diperbarui ketika persediaan berubah atau ketika sumber daya tambahan yang berguna atau baru ditemukan.
- Untuk menanggapi pemberitahuan tentang kerentanan teknis yang relevan, jadwal harus dibuat.
- Setelah mengidentifikasi potensi kerentanan teknis, organisasi harus menentukan risiko dan tindakan korektif yang terkait dengannya. Ini bisa berupa menambal sistem yang rentan atau menerapkan kontrol tambahan.
- Untuk mengkomunikasikan data kerentanan ke fungsi respons insiden dan menyediakan prosedur teknis yang harus dilakukan jika terjadi insiden, proses manajemen kerentanan teknis yang efisien harus diselaraskan dengan aktivitas manajemen insiden.
- Menetapkan prosedur untuk menangani situasi di mana kerentanan telah ditemukan tetapi tidak ada langkah keamanan yang sesuai telah diterapkan. Perusahaan harus menilai risiko yang terkait dengan kerentanan yang teridentifikasi dalam keadaan ini dan menentukan tindakan yang tepat untuk penyelidikan dan perbaikan.

Panduan implementasi 18.2.2 kepatuhan terhadap kebijakan dan standar keamanan

Manajer harus memutuskan bagaimana memeriksa bahwa persyaratan keamanan informasi kebijakan, standar, dan peraturan lain yang berlaku telah terpenuhi. Untuk tinjauan reguler yang efektif, alat pengukuran dan pelaporan otomatis harus dipertimbangkan. Manajer harus mengambil langkah-langkah berikut jika tinjauan mengungkapkan adanya ketidakpatuhan:

- Mencari penyebab ketidakpatuhan
- Melakukan evaluasi apa saja yang dibutuhkan untuk mencapai kepatuhan
- Mengimplementasikan tindakan korektif yang tepat
- memeriksa tindakan korektif yang diambil untuk menentukan kemanjurannya dan menemukan kekurangan atau kekurangan.

Lampiran 3
Pertanyaan

Nama **:** Nansa Sutiono
Jabatan **:** kepala IT

Daftar Pertanyaan

Apakah disini sudah pernah dilakukan penilaian risiko?
jawab: belum pernah

Apakah pernah terjadi gempa bumi pada infrastruktur TI *website* DosenIT?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah tersambar petir?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah kebanjiran?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah kebakaran?
jawab: pernah

Apakah pernah terjadi human error?
jawab: pernah

Apakah pernah terjadi pencurian atau kebocaran data?
jawab: pernah

Apakah pernah terjadi penyalahgunaan hak akses?
jawab: pernah

Apakah pernah terjadi cybercrime?
jawab: pernah

Apakah pernah terjadi data atau informasi tidak sesuai fakta?
jawab: tidak pernah

Apakah mantan pegawai atau user masih memiliki akses data?
jawab: tidak pernah

Apakah pernah terjadi server down?
jawab: pernah

Apakah pernah terjadi kegagalan atau kerusakan hardware?
jawab: pernah

Apakah pernah terjadi sistem crash?
jawab: tidak pernah

Apakah pernah terjadi gagal update?
jawab: tidak pernah

Apakah pernah terjadi *data corrupt*?
jawab: pernah

Apakah pernah terjadi backup gagal?
jawab: pernah

Apakah pernah terjadi *overload*?
jawab: pernah

Apakah pernah koneksi jaringan terputus?
jawab: pernah

Apakah pernah terjadi *Overheat*?
jawab: tidak pernah

Apakah pernah terjadi *Overcapacity*?
jawab: tidak pernah

Apakah pernah terjadi serangan virus atau malware?
jawab: pernah

Nama **:** Eva Yanuarti
Jabatan **:** admin

Daftar Pertanyaan

Apakah pernah terjadi gempa bumi pada infrastruktur TI *website* DosenIT?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah tersambar petir?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah kebanjiran?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah kebakaran?
jawab: pernah

Apakah pernah terjadi *human error*?
jawab: pernah

Apakah pernah terjadi pencurian atau kebocaran data?
jawab: tidak pernah

Apakah pernah terjadi penyalahgunaan hak akses?
jawab: pernah

Apakah pernah terjadi *cybercrime*?
jawab: pernah

Apakah pernah terjadi data atau informasi tidak sesuai fakta?
jawab: tidak pernah

Apakah mantan pegawai atau user masih memiliki akses data?
jawab: tidak pernah

Apakah pernah terjadi server down?
jawab: pernah

Apakah pernah terjadi kegagalan atau kerusakan hardware?
jawab: pernah

Apakah pernah terjadi sistem crash?
jawab: tidak pernah

Apakah pernah terjadi gagal update?
jawab: tidak pernah

Apakah pernah terjadi *data corrupt*?
jawab: pernah

Apakah pernah terjadi backup gagal?
jawab: tidak pernah

Apakah pernah terjadi *overload*?
jawab: pernah

Apakah pernah koneksi jaringan terputus?
jawab: pernah

Apakah pernah terjadi *Overheat*?
jawab: tidak pernah

Apakah pernah terjadi *Overcapacity*?
jawab: tidak pernah

Apakah pernah terjadi serangan virus atau malware?
jawab: pernah

Nama **:** Syifa Lulu Labibah
Jabatan **:** editor

Daftar Pertanyaan

Apakah pernah terjadi gempa bumi pada infrastruktur TI *website* DosenIT?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah tersambar petir?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah kebanjiran?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah kebakaran?
jawab: pernah

Apakah pernah terjadi *human error*?
jawab: pernah

Apakah pernah terjadi pencurian atau kebocaran data?
jawab: tidak pernah

Apakah pernah terjadi penyalahgunaan hak akses?
jawab: tidak pernah

Apakah pernah terjadi *cybercrime*?
jawab: pernah

Apakah pernah terjadi data atau informasi tidak sesuai fakta?
jawab: tidak pernah

Apakah mantan pegawai atau user masih memiliki akses data?
jawab: tidak pernah

Apakah pernah terjadi *server down*?
jawab: pernah

Apakah pernah terjadi kegagalan atau kerusakan hardware?
jawab: pernah

Apakah pernah terjadi sistem crash?
jawab: tidak pernah

Apakah pernah terjadi gagal update?
jawab: tidak pernah

Apakah pernah terjadi *data corrupt*?
jawab: pernah

Apakah pernah terjadi backup gagal?
jawab: tidak pernah

Apakah pernah terjadi *overload*?
jawab: pernah

Apakah pernah koneksi jaringan terputus?
jawab: pernah

Apakah pernah terjadi *Overheat*?
jawab: tidak pernah

Apakah pernah terjadi *Overcapacity*?
jawab: tidak pernah

Apakah pernah terjadi serangan virus atau malware?
jawab: pernah

Nama **:** Nur Aini
Jabatan **:** pengguna

Daftar Pertanyaan

Apakah pernah terjadi gempa bumi pada infrastruktur TI *website* DosenIT?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah tersambar petir?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah kebanjiran?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah kebakaran?
jawab: tidak pernah

Apakah pernah terjadi *human error*?
jawab: pernah

Apakah pernah terjadi pencurian atau kebocaran data?
jawab: tidak pernah

Apakah pernah terjadi penyalahgunaan hak akses?
jawab: tidak pernah

Apakah pernah terjadi *cybercrime*?
jawab: tidak pernah

Apakah pernah terjadi data atau informasi tidak sesuai fakta?
jawab: tidak pernah

Apakah pernah terjadi *server down*?
jawab: pernah

Apakah pernah terjadi kegagalan atau kerusakan hardware?
jawab: tidak pernah

Apakah pernah terjadi sistem crash?
jawab: tidak pernah

Apakah pernah terjadi gagal update?
jawab: tidak pernah

Apakah pernah terjadi *data corrupt*?
jawab: tidak pernah

Apakah pernah terjadi backup gagal?
jawab: tidak pernah

Apakah pernah terjadi *overload*?
jawab: pernah

Apakah pernah koneksi jaringan terputus?
jawab: tidak pernah

Apakah pernah terjadi *Overheat*?
jawab: tidak pernah

Apakah pernah terjadi *Overcapacity*?
jawab: tidak pernah

Apakah pernah terjadi serangan virus atau malware?
jawab: tidak pernah

Nama **:** Tia Melandri
Jabatan **:** pengguna

Daftar Pertanyaan

Apakah pernah terjadi gempa bumi pada infrastruktur TI *website* DosenIT?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah tersambar petir?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah kebanjiran?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah kebakaran?
jawab: tidak pernah

Apakah pernah terjadi *human error*?
jawab: pernah

Apakah pernah terjadi pencurian atau kebocaran data?
jawab: tidak pernah

Apakah pernah terjadi penyalahgunaan hak akses?
jawab: tidak pernah

Apakah pernah terjadi *cybercrime*?
jawab: tidak pernah

Apakah pernah terjadi data atau informasi tidak sesuai fakta?
jawab: tidak pernah

Apakah pernah terjadi *server down*?
jawab: pernah

Apakah pernah terjadi kegagalan atau kerusakan hardware?
jawab: tidak pernah

Apakah pernah terjadi sistem crash?
jawab: tidak pernah

Apakah pernah terjadi gagal update?
jawab: tidak pernah

Apakah pernah terjadi *data corrupt*
jawab: tidak pernah

Apakah pernah terjadi *backup* gagal?
jawab: tidak pernah

Apakah pernah terjadi *overload*?
jawab: tidak pernah

Apakah pernah koneksi jaringan terputus?
jawab: tidak pernah

Apakah pernah terjadi *overheat*?
jawab: tidak pernah

Apakah pernah terjadi *overcapacity*?
jawab: tidak pernah

Apakah pernah terjadi serangan virus atau malware?
jawab: tidak pernah

Apa dampak dari terjadinya human error?
jawab: terdapat typo

Apa dampak dari terjadinya server down?
jawab: saya tidak bisa membuka websitenya

Nama **:** Galih Rakasiwi
Jabatan **:** pengguna

Daftar Pertanyaan

Apakah pernah terjadi gempa bumi pada infrastruktur TI *website* DosenIT?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah tersambar petir?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah kebanjiran?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah kebakaran?
jawab: tidak pernah

Apakah pernah terjadi *human error*?
jawab: pernah

Apakah pernah terjadi pencurian atau kebocaran data?
jawab: tidak pernah

Apakah pernah terjadi penyalahgunaan hak akses?
jawab: tidak pernah

Apakah pernah terjadi *cybercrime*?
jawab: tidak pernah

Apakah pernah terjadi data atau informasi tidak sesuai fakta?
jawab: tidak pernah

Apakah pernah terjadi *server down*?
jawab: tidak pernah

Apakah pernah terjadi kegagalan atau kerusakan hardware?
jawab: tidak pernah

Apakah pernah terjadi sistem crash?
jawab: tidak pernah

Apakah pernah terjadi gagal update?
jawab: tidak pernah

Apakah pernah terjadi *data corrupt*
jawab: tidak pernah

Apakah pernah terjadi *backup* gagal?
jawab: tidak pernah

Apakah pernah terjadi *overload*?
jawab: tidak pernah

Apakah pernah koneksi jaringan terputus?
jawab: tidak pernah

Apakah pernah terjadi *overheat*?
jawab: tidak pernah

Apakah pernah terjadi *overcapacity*?
jawab: tidak pernah

Apakah pernah terjadi serangan virus atau malware?
jawab: tidak pernah

Apa dampak terjadinya human error?
jawab: typo

Nama **:** Kelvin Andrian
Jabatan **:** pengguna

Daftar Pertanyaan

Apakah pernah terjadi gempa bumi pada infrastruktur TI *website* DosenIT?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah tersambar petir?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah kebanjiran?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah kebakaran?
jawab: tidak pernah

Apakah pernah terjadi *human error*?
jawab: pernah

Apakah pernah terjadi pencurian atau kebocaran data?
jawab: tidak pernah

Apakah pernah terjadi penyalahgunaan hak akses?
jawab: tidak pernah

Apakah pernah terjadi *cybercrime*?
jawab: tidak pernah

Apakah pernah terjadi data atau informasi tidak sesuai fakta?
jawab: tidak pernah

Apakah pernah terjadi *server down*?
jawab: tidak pernah

Apakah pernah terjadi kegagalan atau kerusakan hardware?
jawab: tidak pernah

Apakah pernah terjadi sistem crash?
jawab: tidak pernah

Apakah pernah terjadi gagal update?
jawab: tidak pernah

Apakah pernah terjadi *data corrupt*
jawab: tidak pernah

Apakah pernah terjadi *backup* gagal?
jawab: tidak pernah

Apakah pernah terjadi *overload*?
jawab: tidak pernah

Apakah pernah koneksi jaringan terputus?
jawab: tidak pernah

Apakah pernah terjadi *overheat*?
jawab: tidak pernah

Apakah pernah terjadi *overcapacity*?
jawab: tidak pernah

Apakah pernah terjadi serangan virus atau malware?
jawab: tidak pernah

Apa dampak terjadinya human error?
jawab: ada kesalahan dalam ejaan

Nama **:** Nisa Anisa
Jabatan **:** pengguna

Daftar Pertanyaan

Apakah pernah terjadi gempa bumi pada infrastruktur TI *website* DosenIT?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah tersambar petir?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah kebanjiran?
jawab: tidak pernah

Apakah aset TI di *website* DosenIT pernah kebakaran?
jawab: tidak pernah

Apakah pernah terjadi *human error*?
jawab: tidak pernah

Apakah pernah terjadi pencurian atau kebocaran data?
jawab: tidak pernah

Apakah pernah terjadi penyalahgunaan hak akses?
jawab: tidak pernah

Apakah pernah terjadi *cybercrime*?
jawab: tidak pernah

Apakah pernah terjadi data atau informasi tidak sesuai fakta?
jawab: tidak pernah

Apakah pernah terjadi *server down*?
jawab: tidak pernah

Apakah pernah terjadi kegagalan atau kerusakan hardware?
jawab: tidak pernah

Apakah pernah terjadi sistem crash?
jawab: tidak pernah

Apakah pernah terjadi gagal update?
jawab: tidak pernah

Apakah pernah terjadi *data corrupt*
jawab: pernah

Apakah pernah terjadi *backup* gagal?
jawab: tidak pernah

Apakah pernah terjadi *overload*?
jawab: tidak pernah

Apakah pernah koneksi jaringan terputus?
jawab: tidak pernah

Apakah pernah terjadi *overheat*?
jawab: tidak pernah

Apakah pernah terjadi *overcapacity*?
jawab: tidak pernah

Apakah pernah terjadi serangan virus atau malware?
jawab: tidak pernah

Apa dampak dari data corrupt?
jawab: artikelnya tidak ada

Nama **:** Thaufan
Jabatan **:** Tehcnical support ardhosting

Daftar Pertanyaan

Apakah pernah terjadi gempa bumi pada lokasi penyimpanan server?
jawab: tidak pernah

Apakah server pernah tersambar petir?
jawab: tidak pernah

Apakah lokasi penyimpanan server pernah kebanjiran?
jawab: tidak pernah

Apakah lokasi penyimpanan server pernah kebakaran?
jawab: pernah

Apakah pernah terjadi *human error*?
jawab: tidak pernah

Apakah pernah terjadi pencurian atau kebocaran?
jawab: tidak pernah

Apakah pernah terjadi penyalahgunaan hak akses?
jawab: tidak pernah

Apakah mantan pegawai atau user masih memiliki akses data?
jawab: tidak ada

Apakah pernah terjadi *server down*?
jawab: pernah

Apakah pernah terjadi kegagalan atau kerusakan hardware?
jawab: pernah

Apakah pernah terjadi sistem crash?
jawab: tidak pernah

Apakah pernah terjadi gagal update?
jawab: tidak pernah

Apakah pernah terjadi *data corrupt*?
jawab: tidak pernah

Apakah pernah terjadi backup gagal?
jawab: tidak pernah

Apakah pernah terjadi *overload*?
jawab: untuk ini yang mengetahuinya pihak *website*nya

Apakah pernah koneksi jaringan terputus?
jawab: pernah

Apakah pernah terjadi *Overheat*?
jawab: tidak pernah

Apakah pernah terjadi *Overcapacity*?
jawab: untuk ini yang mengetahuinya pihak *website*nya

Apakah pernah terjadi serangan virus atau malware?
jawab: untuk ini yang mengetahuinya pihak *website*nya

Apakah pernah terjadi listrik padam?
jawaba: Pernah

Apakah pernah terjadi tegangan listrik tidak stabil?
jawab: tidak pernah

Apakah pernah terjadi suhu ruangan server tidak stabil?
jawab: pernah

Nama **:** Eva Yanuarti
Jabatan **:** admin

Daftar Pertanyaan

Apa dampak dari terjadinya kebakaran?
jawab: tidak dapat melakukan aktivitas administrasi

Apa dampak dari terjadinya *human error*?
jawab: artikel dihapus

Apa dampak dari terjadinya pencurian atau kebocoran data?
jawab: username dan password tersebar

Apa dampak dari terjadinya penyalahgunaan hak akses?
jawab: dibuatnya artikel yang tidak seharusnya ada seperti promosi situs judi

Apa dampak dari terjadinya *cybercrime*?
jawab: tampilan *website* berubah

Apa dampak dari terjadinya *server down*?
jawab: tidak bisa membuka *website*

Apa dampak dari terjadinya kegagalan atau kerusakan hardware?
jawab: *website* tidak bisa dibuka dan hilangnya data user

Apa dampak dari terjadinya *data corrupt*?
jawab: beberapa artikel tidak dapat dibuka

Apa dampak dari terjadinya *backup* gagal?
jawab: tidak adanya data backup terbaru

Apa dampak dari terjadinya *overload*?
jawab: loadingnya jadi lama

Apa dampak dari terjadinya koneksi jaringan terputus?
jawab: tidak bisa membuka *website*

Apa dampak dari terjadinya serangan virus atau malware?
jawab: beberapa data hilang, baik itu artikel ataupun data user

Nama **:** Syifa Lulu Labibah
Jabatan **:** editor

Daftar Pertanyaan

Apa dampak dari terjadinya kebakaran?
jawab: *website* tidak bisa diakses

Apa dampak dari terjadinya *human error?*
jawab: biasanya user tidak sengaja menghapus artikel

Apa dampak dari terjadinya pencurian atau kebocoran data?
jawab: artikel diambil dari pihak lain

Apa dampak dari terjadinya penyalahgunaan hak akses?
jawab: didalam artikel disisipkan backlink oleh user

Apa dampak dari terjadinya *cybercrime*?
jawab: isi artikel diedit

Apa dampak dari terjadinya *server down*?
jawab: *website* enggk bisa diakses

Apa dampak dari terjadinya kegagalan atau kerusakan hardware?
jawab: *website* enggk bisa diakses

Apa dampak dari terjadinya *data corrupt*?
jawab: artikel tidak bisa diakses

Apa dampak dari terjadinya *backup* gagal?
jawab: tidak adanya backup data

Apa dampak dari terjadinya *overload*?
jawab: *website* sangat sulit untuk diakses

Apa dampak dari terjadinya koneksi jaringan terputus?
jawab: proses publish dan update artikel gagal

Apa dampak dari terjadinya serangan virus atau malware?
jawab: tampilan *website* diubah

Nama **:** Nur Aini
Jabatan **:** pengguna

Daftar Pertanyaan

Apa dampak dari terjadinya *server down*?
jawab: *website* tidak bisa diakses

Apa dampak dari terjadinya *human error*?
jawab: terdapat typo

Apa dampak dari terjadinya *overload*?
jawab: waktu loading menjadi lama

Nama **:** Nansa Sutiono
Jabatan **:** kepala IT

Daftar Pertanyaan

Apa dampak dari terjadinya kebakaran?
jawab: yang pasti hardware kita rusak, beberapa data hilang sama *website*nya tidak bisa diakses

Apa dampak dari terjadinya *human error*?
jawab: paling sering terjadi user menghapus artikel

Apa dampak dari terjadinya pencurian atau kebocoran data?
jawab: kerugian finansial dan data tersebar ke publik

Apa dampak dari terjadinya penyalahgunaan hak akses?
jawab: spam artikel sama spam backlink

Apa dampak dari terjadinya *cybercrime*?
jawab: tampilan *website* diedit

Apa dampak dari terjadinya *server down*?
jawab: *website* lumpuh

Apa dampak dari terjadinya kegagalan atau kerusakan hardware?
jawab: *website* tidak bisa diakses dan terkadang beberapa data hilang karena belum terbackup

Apa dampak dari terjadinya *data corrupt*?
jawab: halaman artikel tidak bisa dibuka, jadi secara otomatis diarahkan ke page not found

Apa dampak dari terjadinya backup gagal?
jawab: tidak adanya backup data terbaru

Apa dampak dari terjadinya *overload*?
jawab: loading *website* jadi sangat lama, terdakang gagal

Apa dampak dari terjadinya koneksi jaringan terputus?
jawab: tidak bisa mengakses *website* DosenIT

Apa dampak dari terjadinya serangan virus atau malware?
jawab: biasanya disisipkan iklan yang ilegal sama tampilan *website* diubah juga

Nama **:** Nansa Sutiono
Jabatan **:** kepala IT

Tabel Keterangan Nilai Kriteria Likelihood

Kriteria	Keterangan	Frekuensi Kejadian
Rare	Kemungkinan Risiko hampir tidak pernah terjadi	>2 tahun
Unlikely	Kemungkinan risiko jarang terjadi	1-2 tahun
Possible	Kemungkinan risiko kadang terjadi	1-12 bulan
Likely	Kemungkinan risiko sering terjadi	4-6 bulan
Certain	Kemungkinan risiko pasti terjadi	1-3 bulan

Daftar Pertanyaan

Seberapa sering terjadinya kebakaran?
jawab: rare

Seberapa sering terjadinya human error?
jawab: likely

Seberapa sering terjadinya penucurian atau kebocoran data?
jawab: rare

Seberapa sering terjadinya penyalahgunaan hak akses?
jawab: possible

Seberapa sering terjadinya cybercrime?
jawab: unlikely

Seberapa sering terjadinya server down?
jawab: unlikely

Seberapa sering terjadinya kegagalan atau kerusakan hardware?
jawab: rare

Seberapa sering terjadinya *data corrupt*?
jawab: unlikely

Seberapa sering terjadinya backup gagal?
jawab: unlikely

Seberapa sering terjadinya *overload*?
jawab: possible

Seberapa sering terjadinya koneksi jaringan terputus?
jawab: unlikely

Seberapa sering terjadinya serangan virus atau malware?
jawab: unlikely

Nama **:** Thaufan
Jabatan **:** technical support ardhosting

Daftar Pertanyaan

Apa dampak terjadinya *server down*?
jawab: web tidak dapat diakses

Apa dampak terjadinya listrik padam?
jawab: server mati

Apa dampak dari suhu ruangan server tidak stabil?
jawab: kinerja server kurangan baik, dalam beberapa kondisi dapat merusak perangkat server

Seberapa sering terjadinya listrik padam?
jawab: Rare

Seberapa sering terjadinya suhu ruangan server tidak stabil?
jawab: Rare

Lampiran 4
Lampiran Tempat Penelitian

Lampiran 5

Universitas Esa Unggul
Fakultas Ilmu Komputer

Jakarta, 1 Desember 2022

Nomor : 83-056/SP/KAPRODI-SI/FASILKOM/UEU/EXT/XII/2022
Lampiran : -
Perihal : ***Surat Permohonan Izin Untuk Penelitian***

Kepada Yth. CEO PT Rio Digital Edutama
Ruko Permata Regency Blok D No. 37,
Jl. Haji Kelik Kelurahan Srengseng,
Kecamatan Kembangan, Jakarta Barat

Dengan hormat,

Sehubungan dengan mata kuliah Tugas Akhir (Skripsi) yang memerlukan data dan informasi bagi mahasiswa Fakultas Ilmu Komputer Program Studi Sistem Informasi, bersama ini kami sampaikan bahwa mahasiswa kami bermaksud untuk mencari beberapa data / informasi. Adapun nama mahasiswa tersebut adalah :

No	NIM	Nama	No HP	Judul Skripsi
1	20190803004	Gilfen Gioferi	085219521010	Penilaian Risiko Teknologi Informasi pada Website Dosen IT Dengan Kerangka Kerja ISO 31000 dan ISO 27002

Kami berharap Bapak/Ibu memberikan izin penelitian untuk Mahasiswa tersebut.

Demikianlah atas perhatian dan kerjasamanya, kami ucapkan terima kasih.

Hormat kami,
Ketua Program Studi Sistem Informasi

Universitas Esa Unggul
Fakultas Ilmu Komputer
Sistem Informasi

Anik Hanifatul Azizah, S.Kom, M.IM

C.c : 1. Arsip
Note : pada saat pengambilan data bisa mengikuti protokol covid (memakai masker, handsanitizer danpengecekan suhu tubuh, dan sangat disarankan untuk mengambil data secara online).