PEMERINTAH KOTA PEKALONGAN
DINAS KOMUNIKASI DAN INFORMATIKA
Jalan Majapahit Nomor : 5 ☎ (0285) 421243 Pekalongan ✉ 51111
Website : http://www.pekalongankota.go.id Email : diskominfo@pekalongankota.go.id

Pekalongan, 6 November 2025

Nomor : B/679.3/500.12.10/2025
Sifat : Biasa
Lampiran : -
Perihal : Undangan

Yth. Tim SMKI
Di

PEKALONGAN

Dengan hormat, dalam rangka meningkatkan pemahaman serta kompetensi terkait pelaksanaan SMKI, maka kami mengundang saudara untuk dapat datang pada :

Hari/Tanggal : Selasa, 11 November 2025
Waktu : 09.00 WIB
Tempat : Ruang Multimedia Dinas Kominfo Kota Pekalongan
Acara : Training Awareness SMKI

Demikian surat ini disampaikan, atas perhatian dan kehadiran Saudara, kami ucapkan terimakasih.

Ditandatangani oleh:
Kepala Dinas Komunikasi dan Informatika Kota Pekalongan

Arif Kanyadi, S.Sos.
NIP. 197110171999031007

Timestamp	Score	Nama Lengkap	Instansi/Perusahaan	Departemen/Bidang	Jabatan
11/11/2025 15.16.41	80 / 100	Candra Agustian Prada	Dinas Kominfo Kota Pekalongan	Bidang Aplikasi dan Persandian	Sandiman Ahli Pertama
11/11/2025 22.08.11	100 / 100	Meidy Prasetyo Utomo	Dinas Kominfo	Bidang APPS	Kepala Seksi Persandian dan
11/13/2025 8.14.35	90 / 100	Elsa mursyidah	dinkominfo	renval / sekretariat	penelaah teknis kebijakan
11/17/2025 9.31.30	100 / 100	Harliyan Tri Mardian	Dinas Kominfo Kota Pekalongan	Bidang aplikasi dan persandian	Pranata komputer ahli pertama
12/5/2025 16.07.39	90 / 100	Amilatul khanief	Dinas Kominfo kota Pekalongan	Sekretariat	Kepala subbagian umum dan
12/5/2025 16.10.36	90 / 100	Agus Arifin	Dinas Komunikasi dan Informatika	Bidang IKP	Pranata Humas Muda
12/5/2025 18.31.44	60 / 100	Prima andana	Dinkominfo kota pekalongan	Sekretariat	Kasubbag
12/6/2025 9.36.26	70 / 100	Rakhmawati, ST	Dinkominfo Kota Pekalongan	Bid APPS	Prakom Ahli Muda
12/7/2025 10.16.59	100 / 100	Suhendri Dwi Prasetyo	Dinas Komunikasi dan Informatika Kota	Infrastruktur dan Statistik	Penata Kelola Sistem dan Teknologi
12/8/2025 7.53.34	100 / 100	Ahmad Ainul, A.Md.Kor	Dinas Komunikasi dan Informatika	Infrastruktur dan Statistik	Pranata Komputer Terampil
12/8/2025 7.59.01	90 / 100	elsa mursyidah	dinkominfo	renval / sekretariat	penelaah teknis kebijakan
12/8/2025 8.01.16	60 / 100	Fahrin Maulana	Dinas Komunikasi dan Informatika Kota	Infrastruktur dan Statistika	Pranata Komputer
12/8/2025 8.53.44	100 / 100	SRI KUDUNG, A.Md.	DINAS KOMINFO KOTA PEKALONGAN	SEKRETARIAT	PRANATA SDM APARATUR
12/10/2025 14.31.17	80 / 100	Fahrin Maulana	Dinas Komunikasi dan Informatika	Bidang Infrastruktur dan Statistika	Pranata Komputer
12/10/2025 14.46.46	100 / 100	Kusuma Adi Achmad	Pemerintah Kota Pekalongan	Bidang Aplikasi dan Persandian	Kepala Bidang Aplikasi dan Persandian
12/10/2025 14.53.46	90 / 100	Muhamad Najib Ferdina	Dinas Komunikasi dan Informatika Kota	Bidang Aplikasi dan Persandian	Penata Kelola Sistem dan Teknologi
12/10/2025 15.52.27	80 / 100	Ainur Rohmah	Dinas Kominfo Kota Pekalongan	Sekretariat	Staf
12/11/2025 8.55.09	60 / 100	GALANG SETIANTO	Dinas Komunikasi dan Informatika Kota	Aplikasi dan Persandian	Pranata Komputer Ahli Pertama
12/11/2025 9.22.13	90 / 100	Zaenal Arifin, A.Md	Dinkominfo	APPS	Pranata Komputer Terampil



TRAINING AWARENESS ISO/IEC 27001:2022
DINAS KOMUNIKASI DAN INFORMATIKA
KOTA PEKALONGAN
2025



Perencanaan Surveillance Sertifikasi ISO 27001:2022

Sistem Manajemen Keamanan Informasi (SMKI)

s.id/presensipretestatpkelongan25

MITRA BERDAYA OPTIMA



Daftar Hadir & Pre-Test

Topik



MITRA BERDAYA OPTIMA

01 PENDAHULUAN

02 PRINSIP SMKI

03 Klausul ISO/IEC 27001:2022

04 Annex ISO/IEC 27001:2022

05 DO’s and DON’Ts

MITRA BERDAYA OPTIMA

Standar ISO/IEC Sistem Manajemen

MITRA BERDAYA OPTIMA

ISO (International Organization for Standardization)

Mengimplementasikan satu standar:

1. ISO/IEC 27001:2022 (SMKI)

Perserikatan badan standarisasi dunia yang bersifat independen. Tujuan mengarahkan organisasi dalam mencapai tujuan.

Format Penomoran

ISO/IEC

Penanda produk dari International Organization for Standardization

27001:

Indeks ISO terkait dengan keamanan informasi

2022

Tahun Revisi



STANDAR ISO
SISTEM MANAJEMEN

Adalah produk yang dikeluarkan oleh ISO untuk membantu organisasi dalam mencapai tujuan organisasi tersebut.

Requirement

Guideline

Code of practice

Sistem Manajemen Keamanan Informasi (SMKI)

Sistem Manajemen Keamanan Informasi (SMKI)

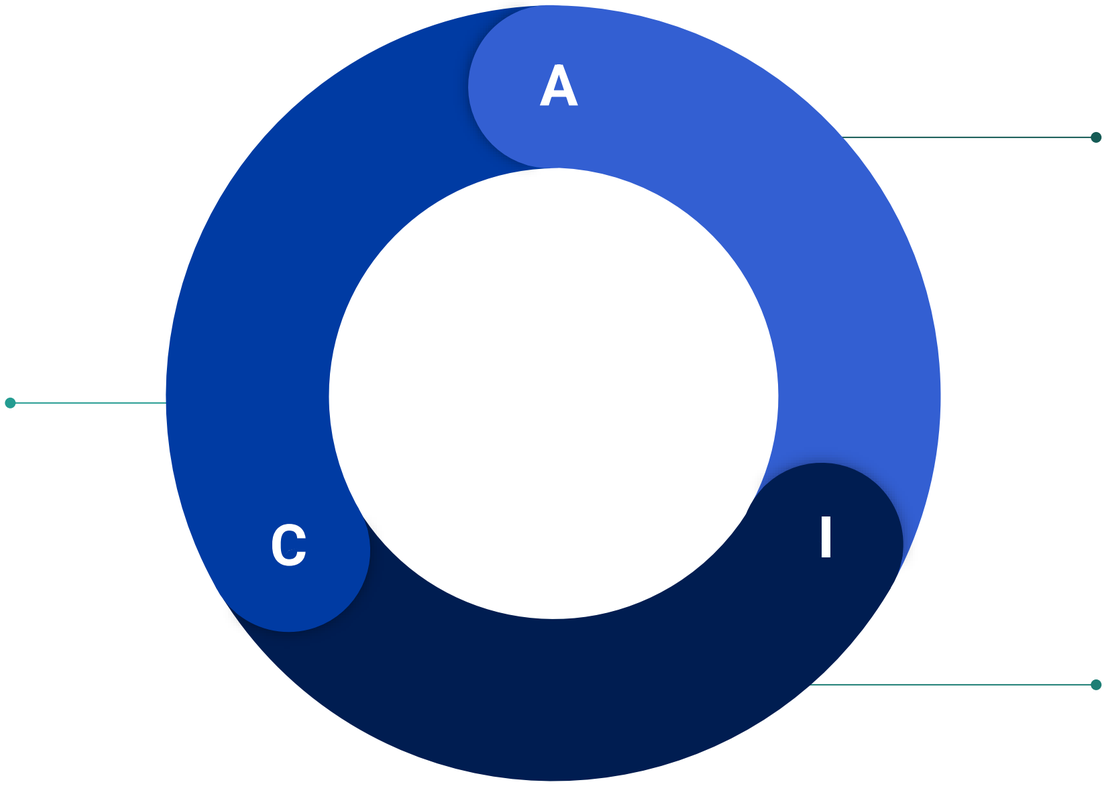
Dalam konteks ISO/IEC 27001:2022, SMKI adalah singkatan dari Sistem Manajemen Keamanan Informasi. ISO/IEC 27001:2022 adalah standar internasional yang memberikan kerangka kerja untuk membangun, menerapkan, memelihara, dan terus meningkatkan sistem manajemen keamanan informasi dalam suatu organisasi.



Prinsip SMKI

Confidentiality
(Kerahasiaan)

Menjamin bahwa informasi hanya dapat diakses oleh orang yang berwenang. Ini melibatkan pengendalian akses dan enkripsi data untuk melindungi informasi dari akses yang tidak sah.



Availability
(Ketersediaan)

Menjamin bahwa informasi dan sistem dapat diakses dan digunakan saat dibutuhkan. Ini mencakup pengelolaan infrastruktur dan pemulihan bencana untuk memastikan layanan tetap tersedia.

Integrity
(Integritas)

Menjamin bahwa informasi akurat dan dapat dipercaya. Ini berarti melindungi data dari modifikasi yang tidak sah atau kehilangan, sehingga informasi tetap utuh dan sesuai dengan keadaan sebenarnya.

Tipe Aset

FISIK

VIRTUAL

INFORMASI

Informasi

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



Manfaat Keamanan Informasi

Pemenuhan Regulasi

Kepatuhan hukum dan kepercayaan masyarakat

Meningkatkan reputasi

Reputasi branding baik

Efisiensi Operasional

Ditingkatkan dengan faktor keamanan informasi

Staff Morale

Ditingkatkan dengan keterlibatan staf dalam keamanan informasi

Fokus Pada SMKI

People	Process	Technology
Memastikan setiap kontribusi untuk keamanan informasi	Memastikan proses pengelolaan terkait efek yang tidak pasti dan dapat mempengaruhi keamanan informasi	Disesuaikan dengan keperluan standar, disesuaikan dengan kemampuan anggaran

Regulasi dan Kepatuhan

Regulasi Terkait:

1. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)
2. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dan Penyelenggaraan Sistem Elektronik
3. Permenkominfo No.20 tahun 2016 Tentang Perlindungan Data Pribadi dalam Sistem Elektronik
4. Undang-undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik
5. Peraturan Menteri Komunikasi dan Digital Nomor 6 Tahun 2025 tentang Standar Teknis dan Prosedur Pembangunan dan Pengembangan Aplikasi Sistem Pemerintahan Berbasis Elektronik
6. Peraturan BSSN No. 9 Tahun 2021 terkait indeks KAMI



MITRA BERDAYA OPTIMA

KLAUSUL ISO/IEC 27001:2022

Klausul ISO/IEC 27001:2022

1. Ruang Lingkup
2. Acuan Normatif
3. Istilah dan Definisi
4. Konteks Organisasi
5. Kepemimpinan
6. Perencanaan
7. Dukungan
8. Operasi
9. Evaluasi Kinerja
10. Kebijakan

Klausul 4 - Konteks Organisasi

4.1 Memahami organisasi dan konteksnya (Isu internal dan isu eksternal)

- Organisasi harus mengidentifikasi isu internal dan eksternal yang relevan dengan tujuan yang mempengaruhi kemampuannya untuk mencapai hasil yang diharapkan dari SMKI Organisasi

4.2 Memahami kebutuhan dan harapan pihak berkepentingan (pihak yang berkepentingan dan persyaratan relevan keamanan informasi)

- Pihak yang berkepentingan yang relevan dengan SMKI
- Ekspektasi dan kebutuhan

Klausul 4 - Konteks Organisasi

4.3 Penentuan ruang lingkup SMKI (Berdasarkan 4.1 dan 4.2)

Dalam penentuan ruang lingkup organisasi harus mempertimbangkan:

1. Isu internal dan eksternal
2. Persyaratan yang dimaksud di 4.2
3. Antarmuka dan dependensi antara aktivitas yang dilakukan oleh organisasi dan aktivitas yang dilakukan oleh organisasi lain.

4.4 Sistem Manajemen Keamanan Informasi

Organisasi harus menetapkan, mengimplementasikan, memelihara, dan meningkatkan secara berkelanjutan sistem manajemen keamanan informasi.

Klausul 5 - Kepemimpinan

5.1 Kepemimpinan dan Komitmen

- Mendukung tercapainya sasaran SMKI
- Integrasi dengan proses bisnis organisasi
- Menyediakan sumberdaya
- Komunikasi persyaratan SMKI
- Memastikan manfaat SMKI
- Memberikan arahan dan dukungan terhadap personel
- Mendorong perbaikan berkelanjutan
- Mendukung manajemen terkait.

Klausul 5 - Kepemimpinan

5.2 Kebijakan

1. Sesuai dengan tujuan organisasi
2. Mencakup sasaran keamanan informasi atau menyediakan kerangka kerja untuk menetapkan sasaran keamanan informasi
3. Mencakup komitmen untuk memenuhi persyaratan yang berlaku terkait dengan keamanan informasi
4. Mencakup komitmen untuk perbaikan berkelanjutan terhadap SMKI

Klausul 5 - Kepemimpinan

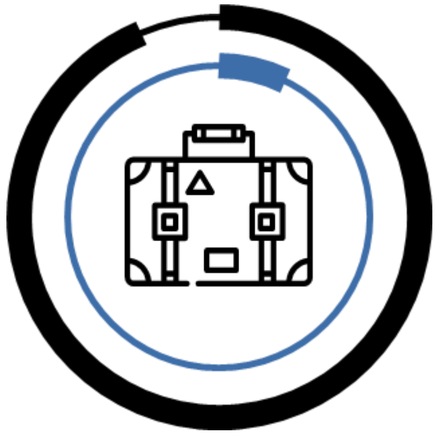
5.3 Peran, Tanggung Jawab, dan Wewenang

Manajemen puncak harus memastikan bahwa tanggung jawab dan wewenang untuk peran yang relevan dengan keamanan informasi ditugaskan dan dikomunikasikan.

Klausul 6 - Perencanaan

6.1 Tindakan Untuk Menangani Risiko dan Peluang

Penilaian Risiko
(Identifikasi, Analisis, Evaluasi)



Penanganan Risiko

Klausul 6 - Perencanaan

6.2 Sasaran Keamanan Informasi dan Perencanaan Untuk Mencapai Sasaran

- Konsisten dengan kebijakan keamanan informasi
- Dapat diukur, dikomunikasikan, dan diperbaharui
- Mempertimbangkan persyaratan keamanan informasi yang berlaku

Klausul 6 - Perencanaan

6.3 Perencanaan Perubahan

Jika organisasi menentukan perlunya perubahan pada Sistem Manajemen Keamanan Informasi maka perubahan itu harus dilakukan secara terencana

Klausul 7 - Dukungan

7.1 Sumber Daya

Untuk penetapan, implementasi, pemeliharaan, dan peningkatan berkelanjutan terhadap SMKI

7.2 Kompetensi

- Menentukan kompetensi yang diperlukan
- Memastikan kompetensi personil
- Mengambil tindakan untuk mendapatkan kompetensi yang diperlukan

7.3 Kepedulian

Kepedulian dan kesadaran mengenai:

- Kebijakan Keamanan Informasi
- Kontribusi terhadap efektivitas SMKI
- Manfaat peningkatan keamanan informasi
- Implikasi dari ketidaksesuaian persyaratan

Klausul 7 - Dukungan

7.4 Komunikasi

- Apa yang dikomunikasikan
- Kapan dikomunikasikan
- Dengan siapa dikomunikasikan
- Siapa yang mengkomunikasikan
- Proses yang dipengaruhi oleh komunikasi
- Bagaimana cara komunikasi

Klausul 7 - Dukungan

7.5 Informasi Terdokumentasi

Informasi terdokumentasi yang ditentukan oleh organisasi sesuai yang diperlukan untuk efektivitas SMKI

7.5.2 Membuat dan Memperbarui Informasi Terdokumentasi

- **Identifikasi dan Deskripsi** (Misal judul, tanggal, penulis, nomor referensi)
- **Format** (Misal bahasa, versi perangkat lunak, grafis)
- **Media** (Misal kertas, elektronik
- **Review dan Persetujuan** (Untuk kesesuaian dan kecukupan)

7.5.3 Pengontrolan Informasi Terdokumentasi

- Tersedia dan cocok untuk digunakan, di mana dan kapan saja diperlukan
- Cukup terlindungi

Klausul 8 - Operasi

8.1 Perencanaan dan Pengendalian Operasi

8.2 Penilaian Risiko Keamanan Informasi

8.3 Penanganan Risiko Keamanan Informasi

Klausul 9 - Evaluasi

9.1 Pemantauan, Pengukuran, Analisis dan Evaluasi

Organisasi harus menentukan:

- **Apa** yang perlu dipantau dan diukur
- **Metode** untuk pemantauan, pengukuran, analisis dan evaluasi
- **Kapan** pemantauan dan pengukuran harus dilakukan
- **Siapa** yang harus memantau dan mengukur
- **Kapan** hasil dari pemantauan dan pengukuran harus dianalisis dan dievaluasi
- **Siapa** yang harus menganalisis dan mengevaluasi hasil tersebut

Klausul 9 - Evaluasi

9.2 Audit Internal

Untuk memastikan bahwa SMKI:

- **Sesuai** dengan persyaratan yang ditetapkan organisasi dan persyaratan Standar ISO/IEC 27001:2022
- **Diimplementasikan dan dipelihara** secara efektif

Klausul 9 - Evaluasi

9.3 Tinjauan Manajemen

- Memastikan kesesuaian, kecukupan dan efektivitas SMKI
- Menghasilkan peluang perbaikan berkelanjutan dan setiap kebutuhan untuk perubahan SMKI

Klausul 10 - Peningkatan

10.1 Peningkatan Berkelanjutan

Organisasi harus terus memperbaiki kesesuaian, kecukupan dan efektivitas SMKI

Klausul 10 - Peningkatan

10.2 Ketidaksesuaian dan Tindakan Korektif

- Bereaksi terhadap ketidaksesuaian
- Mengevaluasi kebutuhan tindakan untuk menghilangkan penyebab ketidaksesuaian, agar hal itu tidak terulang atau terjadi di tempat lain
- Melaksanakan tindakan apapun yang diperlukan
- Mereview efektivitas tindakan korektif
- Membuat perubahan pada SMKI (jika diperlukan)



ANNEX
ISO/IEC 27001:2022

Annex Control



Organization Controls

37 Controls



People Controls

8 Controls



Physical Controls

14 Controls



Technological Controls

34 Controls

Organization Controls

(Kontrol Organisasi)

37 Controls



A.5 - Kontrol Organisasi

Annex 5.1 - Kebijakan Keamanan Informasi

Memberikan arahan dan dukungan manajemen untuk keamanan informasi sesuai dengan persyaratan bisnis dan regulasi dan hukum yang relevan

Dokumen Terkait:

1. Kebijakan Umum SMKI
2. Kebijakan Teknis SMKI

A.5 - Kontrol Organisasi

Annex 5.2 - Peran dan Tanggung Jawab Keamanan Informasi

Menetapkan struktur yang ditetapkan, disetujui dan dipahami untuk implementasi, operasi, dan pengelolaan keamanan informasi dalam organisasi.

Annex 5.3 - Pemisahan Tugas

Tugas dan Tanggung jawab harus dipisahkan oleh Organisasi untuk mengurangi resiko penipuan, kesalahan, dan melewati kontrol keamanan SMKI

Dokumen Terkait:

1. Surat Penunjukan Tim SMKI
2. Surat Penunjukan Tim Audit Internal
3. Prosedur SDM
4. Matrik Kompetensi

A.5 - Kontrol Organisasi

Annex 5.4 - Tanggung Jawab dan Manajemen

Memastikan Manajemen Puncak memahami peran mereka dalam Keamanan Informasi dan memastikan semua personel dalam organisasi mengetahui dan memenuhi tanggung jawab terhadap keamanan informasi di dalam organisasi

Dokumen Terkait:

1. Surat Pernyataan Dukungan Top Manajemen terhadap Penerapan SMKI

A.5 - Kontrol Organisasi

Annex 5.5 - Kontak dengan Pihak Berwenang

Annex 5.6 - Kontak dengan Kelompok Minat Khusus

Organisasi harus membangun dan mempertahankan kontak dengan otoritas terkait, kelompok minat khusus atau forum keamanan khusus lainnya dan asosiasi profesional.

Dokumen Terkait:

1. Daftar Kontak

A.5 - Kontrol Organisasi

Annex 5.7 - Ancaman Kecerdasan

Untuk memberikan kesadaran ancaman lingkungan organisasi, sehingga tindakan mitigasi yang tepat dapat diambil.

Dokumen Terkait:

1. Prosedur Manajemen Insiden
2. Form Manajemen Insiden

A.5 - Kontrol Organisasi

Annex 5.8 - Keamanan Informasi dalam Manajemen Proyek

Untuk memastikan risiko keamanan informasi yang terkait dengan proyek dan hasil kerja ditangani secara efektif dalam manajemen proyek selama siklus proyek berlangsung.

Dokumen Terkait:

1. Prosedur Akuisisi, Pengembangan, dan Perawatan Bisnis

A.5 - Kontrol Organisasi

Annex 5.9 - Inventarisasi Informasi dan Aset

Untuk mengidentifikasi informasi organisasi dan aset terkait lainnya untuk menjaga keamanan informasi organisasi dan menetapkan kepemilikan yang sesuai.

Dokumen Terkait:

1. Prosedur Manajemen Aset
2. Asset Register
3. Form Pemusnahan dan Penggunaan Kembali

A.5 - Kontrol Organisasi

Annex 5.10 - Penggunaan Informasi dan Aset yang Diterima

Untuk memastikan informasi dan aset terkait dilindungi, digunakan, dan ditangani dengan tepat.

Dokumen Terkait:

1. Prosedur Manajemen Aset
2. Asset Register
3. Form Pemusnahan dan Penggunaan Kembali

A.5 - Kontrol Organisasi

Annex 5.11 - Pengembalian Aset

Untuk melindungi aset organisasi sebagai bagian dari proses perubahan atau pemutusan hubungan kerja, kontrak atau perjanjian.

Dokumen Terkait:

1. Prosedur Manajemen Aset
2. Asset Register
3. Form Pemusnahan dan Penggunaan Kembali

A.5 - Kontrol Organisasi

Annex 5.12 - Klasifikasi Informasi

Untuk memastikan identifikasi dan pemahaman kebutuhan perlindungan informasi sesuai dengan kepentingannya bagi organisasi.

Dokumen Terkait:

1. Prosedur Pengendalian Dokumen dan Klasifikasi Informasi
2. Daftar Dokumen Internal
3. Daftar Dokumen Eksternal

Annex 5.13 - Pelabelan Informasi

Untuk memfasilitasi komunikasi klasifikasi informasi dan mendukung otomatisasi pemrosesan dan manajemen informasi.

Dokumen Terkait:

1. Prosedur Manajemen Aset
2. Prosedur Pengendalian Dokumen dan Klasifikasi Informasi
3. Daftar Dokumen Internal
4. Daftar Dokumen Eksternal

A.5 - Kontrol Organisasi

Annex 5.14 - Transfer Informasi

Untuk menjaga keamanan informasi yang ditransfer dalam suatu organisasi dan dengan pihak eksternal yang berkepentingan.

Dokumen Terkait:

1. Prosedur Keamanan Jaringan dan Informasi
2. Prosedur Pengendalian Dokumen dan Klasifikasi Informasi

A.5 - Kontrol Organisasi

Annex 5.15 - Kontrol Akses

Untuk memastikan akses resmi dan untuk mencegah akses tidak sah ke informasi dan aset terkait lainnya

Dokumen Terkait:

1. Prosedur Pengendalian Akses
2. Form Matrik Akses
3. Form Review Akses

A.5 - Kontrol Organisasi

Annex 5.16 - Manajemen Identitas

Untuk identifikasi dari individu dan sistem yang mengakses informasi organisasi beserta aset terkait lainnya dan untuk mengaktifkan hak akses yang tepat.

Dokumen Terkait:

1. Prosedur Pengendalian Akses
2. Form Matrik Akses
3. Form Review Akses

Annex 5.17 - Informasi Autentikasi

Untuk memastikan otentikasi entitas yang tepat dan mencegah kegagalan proses otentikasi.

Dokumen Terkait:

1. Prosedur Pengendalian Akses
2. Prosedur Log-on

Annex 5.18 - Hak Akses

Untuk memastikan akses ke informasi dan aset terkait ditentukan dan disahkan sesuai dengan persyaratan bisnis.

Dokumen Terkait:

1. Prosedur Pengendalian Akses
2. Form Matrik Akses
3. Form Review Akses

A.5 - Kontrol Organisasi

Annex 5.19 - Keamanan Informasi dalam Hubungan Pemasok

Annex 5.20 - Keamanan Informasi dalam Perjanjian Pemasok

Annex 5.21 - Keamanan Informasi dalam Rantai Suplai TIK

Annex 5.22 - Memantau, Meninjau, dan Mengubah Layanan Pemasok

Untuk mempertahankan tingkat keamanan informasi yang disepakati dalam hubungan pemasok sejalan dengan perjanjian.

Dokumen Terkait:

1. Prosedur Keamanan Pemasok
2. Daftar Pemasok
3. Form Seleksi Pemasok
4. Form Evaluasi Pemasok

A.5 - Kontrol Organisasi

Annex 5.23 - Keamanan Informasi untuk Layanan Cloud

Untuk menentukan dan mengelola keamanan informasi untuk penggunaan layanan cloud.

Dokumen Terkait:

1. Prosedur Pengendalian Layanan Cloud
2. Form Checklist Layanan Cloud

A.5 - Kontrol Organisasi

Annex 5.24 - Perencanaan dan Persiapan Manajemen Insiden Keamanan Informasi

Annex 5.25 - Penilaian dan Keputusan Keamanan Informasi

Annex 5.26 - Respon terhadap Insiden Keamanan Informasi

Untuk memastikan respons yang cepat, efektif, konsisten, dan tertib terhadap insiden keamanan informasi, termasuk komunikasi tentang peristiwa keamanan informasi.

Dokumen Terkait:

1. Prosedur Manajemen Insiden
2. Form Pelaporan Insiden

A.5 - Kontrol Organisasi

Annex 5.27 - Pembelajaran dari Insiden Keamanan Informasi

Untuk mengurangi kemungkinan atau konsekuensi dari insiden masa depan.

Dokumen Terkait:

1. Prosedur Manajemen Insiden
2. Form Pelaporan Insiden
3. Form Rekap Insiden

Annex 5.28 - Pengumpulan Bukti

Untuk memastikan pengelolaan bukti yang konsisten dan efektif terkait dengan insiden keamanan informasi untuk tujuan tindakan hukum dan disiplin.

Dokumen Terkait:

1. Prosedur Manajemen Insiden
2. Form Pelaporan Insiden

A.5 - Kontrol Organisasi

Annex 5.29 - Keamanan Informasi Selama Terjadi Gangguan

Annex 5.30 - Kesiapan TIK untuk Kelangsungan Bisnis

Untuk melindungi informasi dan aset terkait lainnya selama gangguan

Dokumen Terkait:

1. Prosedur Keberlangsungan Bisnis dan TIK
2. Rekaman BCP

A.5 - Kontrol Organisasi

Annex 5.31 - Persyaratan Hukum, Perundangan, Peraturan dan Kontrak

Untuk memastikan kepatuhan dengan persyaratan hukum, undang-undang, peraturan dan kontrak yang terkait dengan keamanan informasi.

Dokumen Terkait:

1. Prosedur Kepatuhan
2. Daftar Regulasi

A.5 - Kontrol Organisasi

Annex 5.32 - Hak Kekayaan Intelektual

Untuk memastikan kepatuhan dengan persyaratan hukum, undang-undang, peraturan dan kontrak yang terkait dengan hak kekayaan intelektual dan penggunaan produk hak milik.

Dokumen Terkait:

1. Prosedur Kepatuhan
2. Daftar Regulasi

A.5 - Kontrol Organisasi

Annex 5.33 - Perlindungan dalam Perekaman

Untuk memastikan kepatuhan dengan persyaratan hukum, undang-undang, peraturan dan kontrak, serta harapan komunitas atau masyarakat terkait dengan perlindungan dan ketersediaan rekaman.

Dokumen Terkait:

1. Prosedur Kepatuhan
2. Daftar Regulasi

A.5 - Kontrol Organisasi

Annex 5.34 - Privasi dan Perlindungan PII

Untuk memastikan kepatuhan terhadap persyaratan hukum, undang-undang, peraturan, dan kontrak yang terkait dengan aspek keamanan informasi dari perlindungan PII.

Dokumen Terkait:

1. Prosedur Kepatuhan
2. Daftar Regulasi
3. Kebijakan Privasi

Annex 5.35 - Tinjauan Independen Terhadap Keamanan Informasi

Untuk memastikan kesesuaian, kecukupan dan efektivitas pendekatan organisasi untuk mengelola keamanan informasi.

Dokumen Terkait:

1. Prosedur Kepatuhan
2. Daftar Regulasi
3. Prosedur Audit Internal

A.5 - Kontrol Organisasi

Annex 5.36 - Kepatuhan Terhadap Kebijakan, Peraturan, dan Standar untuk Keamanan Informasi

Untuk memastikan bahwa keamanan informasi diterapkan dan dioperasikan sesuai dengan kebijakan keamanan informasi organisasi, kebijakan, peraturan, dan standar topik khusus.

Dokumen Terkait:

1. Prosedur Kepatuhan
2. Daftar Regulasi
3. Prosedur Audit Internal

A.5 - Kontrol Organisasi

Annex 5.37 - Prosedur Operasi Terdokumentasi

Untuk memastikan pengoperasian fasilitas pemrosesan informasi yang benar dan aman.

Dokumen Terkait:

1. Prosedur Pengendalian Dokumen dan Klasifikasi Informasi
2. Daftar Induk Dokumen
3. Daftar Dokumen Eksternal

People Controls
(Kontrol Sumber Daya Manusia)

8 Controls



A.6 - Kontrol SDM

Annex 6.1 - Screening

Untuk memastikan semua pegawai memenuhi syarat dan sesuai dengan kriteria yang organisasi tetapkan dan tetap memenuhi syarat dan sesuai selama masa kerja pegawai.

Annex 6.2 - Syarat dan Ketentuan Kerja

Untuk memastikan pegawai memahami tanggung jawab keamanan informasi di organisasi sesuai dengan posisi yang organisasi tetapkan.

Dokumen Terkait:

1. Prosedur Manajemen Keamanan Sumber Daya Manusia
2. Form Background Checking Karyawan
3. Form Exit Clearance
4. Peraturan Kedisiplinan

A.6 - Kontrol SDM

Annex 6.3 - Kesadaran, Pembelajaran, dan Pelatihan Keamanan Informasi

Untuk memastikan personel dan pihak terkait yang berkepentingan menyadari dan memenuhi tanggung jawab keamanan informasi.

Dokumen Terkait:

1. Prosedur Peningkatan Awareness dan Komunikasi
2. Form Rencana Pelatihan
3. Matriks Kompetensi

A.6 - Kontrol SDM

Annex 6.4 - Proses Pendisiplinan

Untuk memastikan pegawai dan pihak terkait lainnya yang berkepentingan **memahami konsekuensi dari pelanggaran kebijakan keamanan informasi**, kemudian untuk mencegah dan secara tepat menangani pegawai dan pihak terkait lainnya yang melakukan pelanggaran.

Dokumen Terkait:

1. Prosedur Manajemen Keamanan Sumber Daya Manusia
2. Peraturan Kedisiplinan

A.6 - Kontrol SDM

Annex 6.5 - Tanggung Jawab Setelah Pemutusan Hubungan Kerja atau Perubahan Pekerjaan

Untuk melindungi kepentingan organisasi sebagai bagian dari proses perubahan atau pemutusan hubungan kerja atau kontrak.

Dokumen Terkait:

1. Prosedur Manajemen Keamanan Sumber Daya Manusia
2. Form Exit Clearance

A.6 - Kontrol SDM

Annex 6.6 - Perjanjian Kerahasiaan atau Non-Pengungkapan

Menjaga kerahasiaan informasi yang dapat diakses oleh pegawai atau pihak eksternal.

Dokumen Terkait:

1. Prosedur Keamanan Jaringan dan Informasi
2. Daftar NDA/PKS Karyawan dan Eksternal

A.6 - Kontrol SDM

Annex 6.7 - Kerja Jarak Jauh (Remote Working)

Untuk memastikan keamanan informasi saat pegawai bekerja dari jarak jauh.

Dokumen Terkait:

1. Prosedur Remote Working
2. Form Remote Working

Annex 6.8 - Pelaporan Insiden Keamanan Informasi

Untuk mendukung pelaporan insiden keamanan informasi yang tepat waktu, konsisten, dan efektif yang dapat diidentifikasi oleh pegawai.

Dokumen Terkait:

1. Prosedur Manajemen Insiden
2. Form Pelaporan Insiden

Physical Controls

(Kontrol Fisik)

14 Controls



A.7 - Kontrol Fisik

Annex 7.1 - Batas Keamanan Fisik

Untuk mencegah akses fisik yang tidak sah, kerusakan dan gangguan terhadap informasi organisasi dan aset terkait lainnya.

Annex 7.2 - Akses Masuk

Untuk memastikan hanya akses resmi yang masuk ke informasi organisasi dan aset terkait lainnya.

Annex 7.3 - Pengamanan Kantor, Ruangan, dan Fasilitas

Untuk mencegah akses fisik yang tidak sah, kerusakan dan gangguan terhadap informasi organisasi dan aset terkait lainnya di kantor, ruangan, dan fasilitas.

Dokumen Terkait:

1. Zonasi kantor dan denahnya
2. Prosedur Keamanan Area Fisik

A.7 - Kontrol Fisik

Annex 7.4 - Pemantauan Keamanan Fisik

Untuk mendeteksi dan mencegah akses fisik yang tidak sah.

Dokumen Terkait:

1. Zonasi kantor dan denahnya
2. Prosedur Keamanan Area Fisik

Annex 7.5 - Perlindungan dari Ancaman Fisik dan Lingkungan

Untuk mencegah atau mengurangi konsekuensi dari insiden yang berasal dari ancaman fisik dan lingkungan.

Dokumen Terkait:

1. Prosedur Keamanan Area Fisik

A.7 - Kontrol Fisik

Annex 7.6 - Bekerja di Area Aman

Untuk melindungi informasi dan aset terkait lainnya di area aman dari kerusakan dan gangguan tidak sah/ilegal oleh pegawai yang bekerja di area tersebut.

Dokumen Terkait:

1. Prosedur Keamanan Area Fisik
2. Denah Kantor

A.7 - Kontrol Fisik

Annex 7.7 - Bersihkan Meja dan Bersihkan Layar

Untuk mengurangi risiko akses tidak sah, kehilangan dan kerusakan informasi di meja, layar, dan di lokasi lain yang dapat diakses selama dan di luar jam kerja normal.

Dokumen Terkait:

1. Prosedur Keamanan Area Fisik

A.7 - Kontrol Fisik

Annex 7.8 - Penempatan Peralatan dan Perlindungan

Untuk mengurangi risiko dari ancaman fisik dan lingkungan, dan dari akses yang tidak sah.

Dokumen Terkait:

1. Prosedur Manajemen Aset

Annex 7.9 - Keamanan Aset di Luar Lokasi

Untuk mencegah kehilangan, kerusakan, pencurian, atau penyusupan perangkat di luar lokasi dan gangguan pada operasi organisasi.

Dokumen Terkait:

1. Prosedur Keamanan Area Fisik

Annex 7.10 - Media Penyimpanan

Untuk memastikan hanya pengungkapan yang resmi, modifikasi, penghapusan atau penghancuran informasi yang sah pada media penyimpanan.

Dokumen Terkait:

1. Prosedur Manajemen Aset

A.7 - Kontrol Fisik

Annex 7.11 - Utilitas Pendukung

Untuk mencegah kehilangan, kerusakan atau kompromi informasi dan aset terkait lainnya, atau gangguan pada operasi organisasi karena kegagalan dan gangguan utilitas pendukung.

Dokumen Terkait:

1. Prosedur Manajemen Aset
2. Prosedur Perawatan Utilitas
3. Rekaman Pemeliharaan Utilitas

A.7 - Kontrol Fisik

Annex 7.12 - Keamanan Kabel

Untuk mencegah kehilangan, kerusakan, pencurian, atau penyusupan informasi dan aset terkait lainnya serta gangguan pada operasi organisasi terkait dengan kabel daya dan komunikasi.

Dokumen Terkait:

1. Prosedur Manajemen Aset
2. Prosedur Perawatan Utilitas
3. Prosedur Maintenance Aset

A.7 - Kontrol Fisik

Annex 7.13 - Pemeliharaan Peralatan

Untuk mencegah kehilangan, kerusakan, pencurian atau kompromi informasi dan aset terkait lainnya serta gangguan terhadap operasi organisasi yang disebabkan oleh kurangnya pemeliharaan.

Dokumen Terkait:

1. Prosedur Manajemen Aset
2. Prosedur Perawatan Utilitas
3. Prosedur Maintenance Aset

A.7 - Kontrol Fisik

Annex 7.14 - Pembuangan atau Penggunaan Kembali Peralatan yang Aman

Untuk mencegah kebocoran informasi dari peralatan yang akan dibuang atau digunakan kembali.

Dokumen Terkait:

1. Prosedur Manajemen Aset
2. Form Aset Register
3. Form Pemusnahan dan Penggunaan Kembali

Technological Controls

(Kontrol Teknologi)

34 Controls



A.8 - Kontrol Teknologi

Annex 8.1 - Perangkat Endpoint Pengguna

Untuk melindungi informasi terhadap risiko yang ditimbulkan dengan menggunakan perangkat endpoint pengguna.

Dokumen Terkait:

1. Form BYOD
2. Prosedur BYOD
3. Asset Register
4. Form Monitoring Malware

A.8 - Kontrol Teknologi

Annex 8.2 - Hak Akses Istimewa

Untuk memastikan hanya pengguna yang berwenang, komponen perangkat lunak dan layanan disediakan dengan hak akses istimewa.

Annex 8.3 - Pembatasan Akses Informasi

Untuk memastikan hanya akses resmi dan untuk mencegah akses tidak sah ke informasi dan lainnya

Annex 8.4 - Akses Ke Kode Sumber

Untuk mencegah masuknya fungsionalitas yang tidak sah, menghindari perubahan yang tidak disengaja atau berbahaya dan untuk menjaga kerahasiaan kekayaan intelektual yang berharga.

Dokumen Terkait:

1. Prosedur Pengendalian Akses
2. Form Matriks Akses
3. Form Review Akses

A.8 - Kontrol Teknologi

Annex 8.5 - Otentikasi Aman

Untuk memastikan pengguna atau entitas diautentikasi dengan aman, saat akses ke sistem, aplikasi, dan layanan yang diberikan.

Dokumen Terkait:

1. Prosedur Pengendalian Akses
2. Prosedur Log-On

A.8 - Kontrol Teknologi

Annex 8.6 - Manajemen Kapasitas

Untuk memastikan kapasitas yang diperlukan fasilitas pengolahan informasi, sumber daya manusia, kantor dan fasilitas lainnya.

Dokumen Terkait:

1. Prosedur Manajemen Kapasitas dan Backup
2. Rekaman Review Kapasitas

A.8 - Kontrol Teknologi

Annex 8.7 - Perlindungan Terhadap Malware

Untuk memastikan informasi dan aset terkait lainnya terlindungi dari malware.

Dokumen Terkait:

1. Prosedur Operasional Teknis
2. Form Kendali Malware

A.8 - Kontrol Teknologi

Annex 8.8 - Manajemen Kerentanan Teknis

Untuk mencegah eksploitasi terhadap kerentanan teknis.

Dokumen Terkait:

1. Prosedur Penetration Testing
2. Hasil Pentest
3. Prosedur Audit Internal (Program Audit, Checklist Audit, Rencana Audit)

A.8 - Kontrol Teknologi

Annex 8.9 - Manajemen Konfigurasi

Untuk memastikan perangkat keras, perangkat lunak, layanan, dan jaringan berfungsi dengan benar dengan pengaturan keamanan yang diperlukan, dan konfigurasi tidak diubah oleh perubahan yang tidak sah atau salah.

Dokumen Terkait:

1. Prosedur Log-On
2. Form Matrik Akses
3. Prosedur Pengendalian Akses

A.8 - Kontrol Teknologi

Annex 8.10 - Penghapusan Informasi

Untuk mencegah pengungkapan informasi sensitif yang tidak perlu dan untuk mematuhi persyaratan hukum, undang-undang, peraturan, dan kontrak untuk penghapusan informasi.

Dokumen Terkait:

1. Prosedur Pengendalian Dokumen

Annex 8.11 - Penyembunyian Data

Untuk membatasi pemaparan data sensitif termasuk PII, dan untuk mematuhi persyaratan hukum, undang-undang, peraturan, dan kontrak.

Dokumen Terkait:

1. Prosedur Pengendalian Dokumen

A.8 - Kontrol Teknologi

Annex 8.12 - Pencegahan Kebocoran Data

Untuk mendeteksi dan mencegah pengungkapan dan pemisahan informasi yang tidak sah oleh individu atau sistem.

Dokumen Terkait:

1. Peraturan Perundang-Undangan
2. NDA/PKS Karyawan
3. Pengendalian Akses

A.8 - Kontrol Teknologi

Annex 8.13 - Pencadangan Informasi

Untuk mengaktifkan pemulihan dari kehilangan data atau sistem.

Dokumen Terkait:

1. Prosedur Manajemen Kapasitas dan Backup
2. Form Review Backup dan Rekaman Backup
3. Form Review Restore dan Rekaman Restore

Annex 8.14 - Redundansi Fasilitas Pemrosesan Informasi

Untuk memastikan pengoperasian berkelanjutan dari fasilitas pemrosesan informasi.

Dokumen Terkait:

1. Prosedur Manajemen Keberlangsungan Bisnis

A.8 - Kontrol Teknologi

Annex 8.15 - Logging

Untuk merekam peristiwa, menghasilkan bukti, memastikan integritas informasi log, mencegah akses tidak sah, mengidentifikasi peristiwa keamanan informasi yang dapat menyebabkan insiden keamanan informasi dan mendukung penyelidikan.

Dokumen Terkait:

1. Prosedur Log-on dan Monitoring
2. Form Review Log
3. Rekaman Log

A.8 - Kontrol Teknologi

Annex 8.16 - Kegiatan Pemantauan

Untuk mendeteksi perilaku yang bertentangan dan potensi insiden keamanan informasi.

Dokumen Terkait:

1. Prosedur Logging dan Monitoring
2. Form Review Log
3. Rekaman Log

A.8 - Kontrol Teknologi

Annex 8.17 - Sinkronisasi Jam

Untuk mengaktifkan korelasi dan analisis peristiwa terkait keamanan dan data terekam lainnya, dan untuk mendukung investigasi terhadap insiden keamanan informasi.

Dokumen Terkait:

1. Prosedur Operasional Teknis

Annex 8.18 - Penggunaan Program Utilitas Istimewa

Untuk memastikan penggunaan program utilitas tidak membahayakan kontrol sistem dan aplikasi untuk keamanan informasi.

Dokumen Terkait:

1. Prosedur Manajemen Akses

Annex 8.19 - Instalasi Perangkat Lunak Pada Sistem Operasional

Untuk memastikan integritas sistem operasional dan mencegah pendayagunaan terhadap kerentanan teknis.

Dokumen Terkait:

1. Prosedur Pengelolaan Software dan Aplikasi
2. Software Whitelist

A.8 - Kontrol Teknologi

Annex 8.20 - Keamanan Jaringan

Untuk melindungi informasi dalam jaringan dan fasilitas pemrosesan informasi pendukungnya dari kompromi melalui jaringan.

Dokumen Terkait:

1. Prosedur Keamanan Jaringan dan Komunikasi
2. Arsitektur Jaringan Kantor
3. Arsitektur Jaringan Cloud

A.8 - Kontrol Teknologi

Annex 8.21 - Keamanan Layanan Jaringan

Untuk menjamin keamanan dalam penggunaan layanan jaringan

Annex 8.22 - Pemisahan Jaringan

Untuk membagi jaringan dalam batas-batas keamanan dan untuk mengontrol lalu lintas di jaringan berdasarkan kebutuhan bisnis

Dokumen Terkait:

1. Prosedur Keamanan Jaringan dan Komunikasi
2. Arsitektur Jaringan Kantor
3. Arsitektur Jaringan Cloud

A.8 - Kontrol Teknologi

Annex 8.23 - Penyaringan Web

Akses ke situs web eksternal harus dikelola untuk mengurangi paparan konten berbahaya.

Dokumen Terkait:

1. Prosedur Keamanan Jaringan dan Komunikasi/Prosedur Akses Web
2. List Of web Filtering

A.8 - Kontrol Teknologi

Annex 8.24 - Penggunaan Kriptografi

Untuk memastikan penggunaan kriptografi yang tepat dan efektif untuk melindungi kerahasiaan, keaslian, atau integritas informasi sesuai dengan kebutuhan bisnis dan keamanan informasi, dan dengan mempertimbangkan persyaratan hukum, undang-undang, peraturan, dan kontrak yang terkait dengan kriptografi.

Dokumen Terkait:

1. Prosedur Kriptografi
2. Daftar kriptografi

A.8 - Kontrol Teknologi

Annex 8.25 - Siklus Pengembangan yang Aman

Untuk memastikan keamanan informasi dirancang dan diimplementasikan dalam siklus hidup pengembangan perangkat lunak dalam sistem yang aman.

Dokumen Terkait:

1. Prosedur Akuisisi, Pengembangan dan Perawatan Sistem
2. Prosedur Siklus Pengembangan Sistem (SDLC)

A.8 - Kontrol Teknologi

Annex 8.26 - Persyaratan Keamanan Aplikasi

Untuk memastikan semua persyaratan keamanan informasi diidentifikasi dan ditangani saat mengembangkan atau memperoleh aplikasi.

Dokumen Terkait:

1. Prosedur Akuisisi, Pengembangan dan Perawatan Sistem

A.8 - Kontrol Teknologi

Annex 8.27 - Arsitektur Sistem yang Aman dan Prinsip-Prinsip Rekayasa

Untuk memastikan sistem informasi dirancang, diimplementasikan, dan dioperasikan dengan aman dalam siklus hidup pengembangan.

Dokumen Terkait:

1. Prosedur Pengkodean yang Aman

A.8 - Kontrol Teknologi

Annex 8.28 - Pengkodean Aman

Untuk memastikan perangkat lunak dibuat dengan aman sehingga mengurangi jumlah potensi kerentanan keamanan informasi dalam perangkat lunak

Dokumen Terkait:

1. Prosedur Pengkodean Yang Aman
2. Prosedur Akuisisi, Pengembangan dan Perawatan Sistem
3. Prosedur Siklus Pengembangan Sistem (SDLC)
4. Form RFC (Request For Change)

A.8 - Kontrol Teknologi

Annex 8.29 - Pengujian Keamanan dalam Pengembangan dan Penerimaan

Untuk memvalidasi apakah persyaratan keamanan informasi terpenuhi saat aplikasi atau kode disebarkan ke lingkungan organisasi.

Dokumen Terkait:

1. Prosedur Akuisisi, Pengembangan dan Perawatan Sistem
2. Prosedur Pengkodean yang Aman
3. Rekaman pengujian sistem

A.8 - Kontrol Teknologi

Annex 8.30 - Pengembangan Outsourcing

Untuk memastikan langkah-langkah keamanan informasi yang diperlukan oleh organisasi diimplementasikan dalam pengembangan sistem outsourcing.

Dokumen Terkait:

1. Prosedur Akuisisi, Pengembangan dan Perawatan Sistem
2. Prosedur Pengkodean Aman

A.8 - Kontrol Teknologi

Annex 8.31 - Pemisahan Lingkungan Pengembangan, Pengujian, dan Produksi

Untuk melindungi lingkungan produksi dan data dari kompromi oleh aktivitas pengembangan dan pengujian.

Dokumen Terkait:

1. Prosedur Akuisisi, Pengembangan dan Perawatan Sistem
2. Prosedur Pengkodean Aman

A.8 - Kontrol Teknologi

Annex 8.32 - Manajemen Perubahan

Untuk menjaga keamanan informasi saat menjalankan perubahan.

Dokumen Terkait:

1. Prosedur Manajemen Perubahan
2. Form RFC (Request For Change)
3. Rekap RFC
4. Prosedur Akuisisi, Pengembangan dan Perawatan Sistem
5. Rekaman perubahan sistem
6. Report Pentest

A.8 - Kontrol Teknologi

Annex 8.33 - Informasi Pengujian

Untuk memastikan relevansi pengujian dan perlindungan informasi operasional yang digunakan untuk pengujian.

Dokumen Terkait:

1. Prosedur Akuisisi, Pengembangan dan Perawatan Sistem
2. Report Pentest

Annex 8.34 - Perlindungan Sistem Informasi Selana Pengujian Audit

Meminimalkan dampak audit dan aktivitas assurance lainnya terhadap sistem operasional dan proses bisnis.

Dokumen Terkait:

1. Prosedur Operasional Teknis

MITRA BERDAYA OPTIMA

Dokumen Yang Diperlukan

Dokumen Integrasi

Dokumen Terkait:

1. Pengendalian dokumen
2. Kebijakan keamanan informasi
3. Tim SMKI
4. Ruang lingkup SMKI
5. Sasaran Keamanan Informasi
6. Sumber daya, kompetensi, awareness, komunikasi
7. Manajemen risiko
8. Audit internal
9. Tinjauan manajemen
10. Penanganan ketidaksesuaian dan peningkatan
11. Proses bisnis



Dokumen Teknis

Dokumen Terkait:

0. Statement of Applicability
1. Keamanan SDM
2. Klasifikasi informasi
3. Pengamanan perangkat keras
4. Manajemen aset
5. Kendali akses
6. Pengamanan area fisik
7. Pengelolaan perangkat lunak
8. Manajemen perubahan
9. Manajemen kapasitas dan backup
10. Logging informasi
11. Manajemen kerentanan teknis
12. Keamanan jaringan dan komunikasi
13. Akuisisi pengembangan perawatan sistem
14. Pengamanan pemasok
15. Manajemen insiden
16. Keberlanjutan bisnis dan TIK
17. Kepatuhan Keamanan Informasi
18. Kontak pihak berwenang dan kelompok minat khusus
19. Pengendalian Layanan Cloud
20. Remote Working
21. Perawatan Utilitas dan Maintenance Aset
22. Pengelolaan Software dan Aplikasi
23. Akses Web dan Pengkodean yang Aman

MITRA BERDAYA OPTIMA

Persiapan Audit Eksternal

Pastikan!

- Semua **dokumen, SOP, dan form** sudah **lengkap** dan **disahkan pimpinan**.
- **Semua perangkat** telah **disetting sesuai dengan prosedur** yang ditetapkan (seperti password/pin disesuaikan)

MITRA BERDAYA OPTIMA

DO’s dan DON’Ts

- Patuhi kebijakan keamanan informasi yang berlaku di organisasi dan perlakukan informasi sebagai aset.
- Lakukan proses penyaringan sumber daya manusia yang memadai dan pastikan adanya perjanjian kerahasiaan dengan karyawan, pemasok, maupun pihak ketiga lainnya (non-disclosure agreement, NDA)
- Ikuti prosedur pengendalian akses, patuhi aturan penggunaan akun dan password, serta gunakan enkripsi bilamana diperlukan
- Dokumentasikan proses operasional dan pastikan adanya cadangan informasi yang memadai (backup)
- Pastikan kesiapan operasional organisasi dalam menghadapi ancaman dengan menyusun rencana keberlangsungan bisnis (business continuity plan, BCP)
- Pastikan kesesuaian penerapan sistem manajemen keamanan informasi dengan hukum dan peraturan yang berlaku
- Lakukan monitoring dan audit keamanan informasi baik secara mandiri maupun melalui program audit secara khusus





MITRA BERDAYA OPTIMA

Tidak Boleh Dilakukan

- Jangan mengakses informasi terkait pekerjaan di tempat yang tidak aman atau menggunakan jaringan yang tidak terjamin keamanannya.
- Hindari penggunaan media portable yang tidak teregistrasi seperti USB Flashdisk, hard-disk eksternal, smartphone, tablet, dll.
- Jangan meninggalkan laptop / workstation tanpa mengunci layar dan jangan meninggalkan dokumen fisik di atas meja tanpa pengawasan
- Jangan menggunakan perangkat lunak yang tidak berlisensi atau tidak masuk ke dalam white-list organisasi
- Jangan berbagi akun untuk mengakses informasi
- Jangan mengubah konfigurasi perangkat, jaringan, dan perangkat lunak tanpa adanya proses manajemen perubahan terlebih dahulu
- Jangan membiarkan hal-hal yang berpotensi menjadi insiden. Laporkan setiap kerentanan dan potensi insiden keamanan informasi pada tim SMKI organisasi.

s.id/posttesttapkealongan25



MITRA BERDAYA OPTIMA

Post-Test

MITRA
BERDAYA
OPTIMA

TERIMA KASIH

Contact Us

www.mitraberdaya.id

contact@mitraberdaya.id