Sosialisasi Kebijakan

SNI ISO/IEC 27001:2022

Sistem Manajemen Keamanan Informasi

MBO MITRA BERDAYA OPTIMA

MITRA BERDAYA OPTIMA

SISTEM MANAJEMEN

Sistem manajemen adalah arahan baku yang disusun untuk membantu dalam menjalankan suatu pekerjaan dengan tanpa kesalahan atau dengan kesalahan yang minimal.

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.

MITRA BERDAYA OPTIMA

KASUS KEBOCORAN DATA

MITRA BERDAYA OPTIMA

KEAMANAN INFORMASI

1. Keamanan informasi tercapai apabila **kerahasiaan, integritas,** dan **ketersediaan** dari informasi terpenuhi.
2. Penerapan keamanan informasi menggunakan **Risk Based Thinking**

Note: Sistem manajemen termasuk struktur organisasi, kebijakan, prosedur, proses, dan sumberdaya.

PRINSIP CIA

CONFIDENTIALITY

Informasi hanya dapat diakses oleh orang yang berhak atau pihak yang berwenang.

INTEGRITY

Memastikan keakuratan dan kelengkapan informasi termasuk metode pemrosesan informasi yang digunakan

AVAILABILITY

Memastikan informasi tersedia ketika dibutuhkan oleh pihak yang berwenang

SNI ISO/IEC 27001:2022

ISO/IEC

International organization for Standardization (ISO) merupakan perserikatan badan-badan standardisasi dunia.

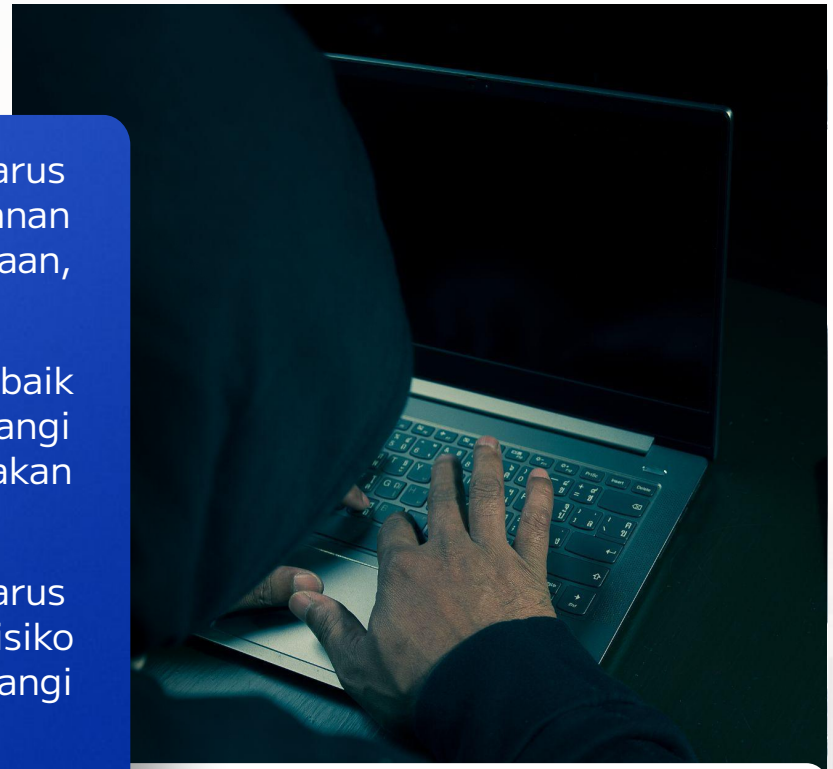
27001

Kode 27001 merupakan standar untuk Sistem Manajemen Keamanan Informasi

2022

Standar untuk Sistem Manajemen Keamanan Informasi versi revisi 2022

KONSEP SMKI



- Dinas Komunikasi dan Informatika Kabupaten Kudus harus menetapkan dan menerapkan kebijakan keamanan informasi yang jelas untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi.
- pegawai harus dilatih dan memiliki kesadaran yang baik tentang praktik keamanan informasi untuk mengurangi risiko kesalahan manusia yang dapat membahayakan informasi.
- Dinas Komunikasi dan Informatika Kabupaten Kudus harus mengidentifikasi, menganalisis, dan mengelola risiko keamanan informasi dengan tujuan untuk mengurangi risiko ke tingkat yang dapat diterima.

MITRA BERDAYA OPTIMA

Perluasan dari SNI ISO/IEC 27001

SNI ISO/IEC 27701 dibangun di atas kerangka SNI ISO/IEC 27001, yang berarti Dinas Komunikasi dan Informatika Kabupaten Kudus yang sudah memiliki ISMS berdasarkan SNI ISO/IEC 27001 dapat memperluasnya untuk mencakup pengelolaan privasi dengan mengikuti ISO/IEC 27701.

SNI ISO 27001

Memastikan keamanan aset informasi (C-I-A)

MANFAAT PENERAPAN SMKI

- Peningkatan keamanan dan mengurangi risiko terjadinya insiden keamanan informasi.
- Peningkatan kepatuhan terhadap regulasi yang berlaku.
- Peningkatan kesadaran terkait keamanan informasi dalam proses operasi dan layanan.
- Peningkatan reputasi dan kepercayaan berdasarkan komitmen lembaga terhadap keamanan informasi.

Kebijakan Umum

1. Informasi merupakan salah satu aset utama dalam setiap kegiatan yang diselenggarakan oleh Dinas Komunikasi dan Informatika Kabupaten Kudus. Oleh karena itu, kerahasiaan (confidentiality), kebenaran (integrity), dan ketersediaan (availability) informasi perlu dikelola sehingga keamanannya dapat terjaga.
2. Penerapan sistem manajemen keamanan informasi di Dinas Komunikasi dan Informatika Kabupaten Kudus mengacu pada standar SNI ISO/IEC 27001:2022 dan peraturan perundang-undangan yang berlaku.
3. Kepala Dinas Komunikasi dan Informatika Kabupaten Kudus senantiasa menunjukkan kepemimpinan dan komitmen untuk menerapkan keamanan informasi di Dinas Komunikasi dan Informatika Kabupaten Kudus
4. Kebijakan keamanan informasi harus dikomunikasikan ke seluruh pegawai dan pihak eksternal yang terkait melalui media komunikasi yang ada agar dapat dengan mudah dipahami dan dipatuhi.

Kebijakan Umum

5. Dinas Komunikasi dan Informatika Kabupaten Kudus akan selalu berusaha meningkatkan kepedulian (awareness), pengetahuan, dan keterampilan tentang keamanan informasi bagi pegawai maupun pihak eksternal yang terkait.
6. Dinas Komunikasi dan Informatika Kabupaten Kudus melaksanakan kajian dan mengelola risiko-risiko terkait keamanan informasi dan keamanan privasi berdasarkan kerentanan (vulnerability) dan ancaman (threat) yang ada pada setiap aset maupun proses.
7. Jika terdapat kerentanan dan ancaman yang berpotensi mengganggu keamanan informasi, maka semua pihak yang berkepentingan wajib melaporkannya kepada Ketua Tim SMKI atau anggota Tim SMKI.
8. Seluruh pimpinan di semua tingkatan bertanggung jawab memantau dan mengevaluasi efektivitas penerapan kebijakan ini di seluruh unit kerja/bagian di bawah pengawasannya sebagai komitmen dalam peningkatan berkelanjutan.

Kebijakan Umum

9. Seluruh pegawai bertanggung jawab untuk menjaga dan melindungi keamanan aset informasi serta mematuhi kebijakan dan prosedur keamanan informasi dan keamanan privasi yang telah ditetapkan.
10. Setiap pelanggaran terhadap kebijakan ini dan kebijakan lain yang terkait akan dikenai sanksi administratif seperti pencabutan hak akses sistem informasi dan/atau tindakan pendisiplinan lain sesuai peraturan yang berlaku
11. Dinas Komunikasi dan Informatika Kabupaten Kudus berkomitmen untuk terus melakukan perbaikan berkelanjutan terhadap implementasi Sistem Manajemen Keamanan Informasi.

Manajemen Risiko

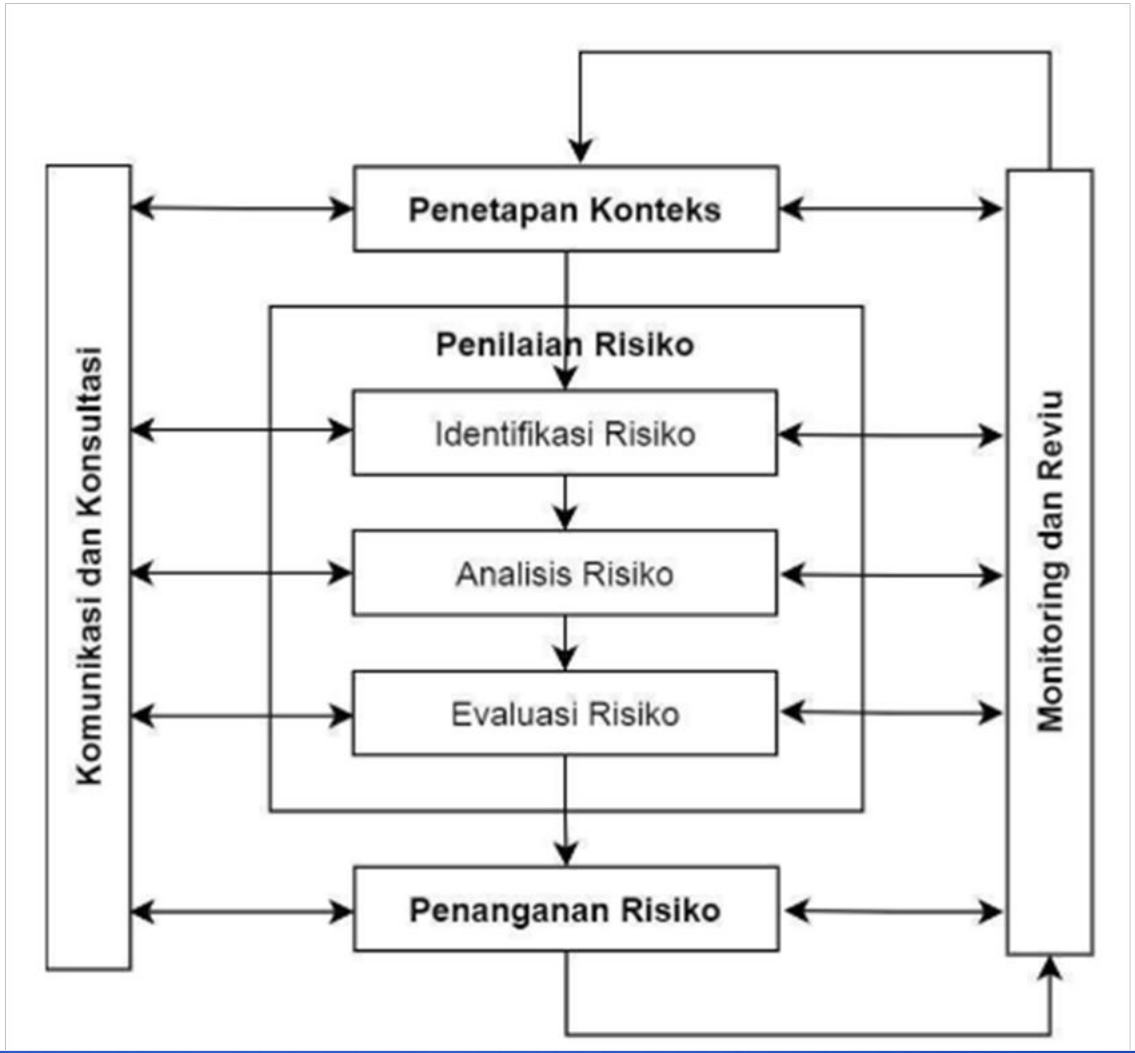
Organisasi harus merencanakan tindakan untuk mengatasi risiko dan peluang

- **Risiko**: dihindari, dikendalikan, diambil, mengurangi kemungkinannya, berbagi risiko, dll.
- **Peluang**: seberapa organisasi mengetahui peluang dalam mengetahui/mengenali risiko dan mengurangi risiko setelah teridentifikasi.
- Mengevaluasi efektifitas tindakan

Peluang dapat mengarah pada

- Adopsi praktik baru;
- Mendorong Inovasi;
- Peningkatan Kepatuhan;
- Meningkatkan Efisiensi Operasional;
- Membangun kemitraan;
- Memperbaiki Reputasi;
- Menggunakan teknologi baru dan keinginan lain, serta
- Kelayakan untuk memenuhi kebutuhan organisasi atau pelanggan

BUSINESS RISK ASSESSMENT PROCESS



MANAJEMEN ASET

Siapa yang bertanggung jawab?

Metode Pelabelan

Inventori Aset

Tipe aset

Pengembalian /penggunaan Kembali/Peng hapusan aset

Tipe Aset

- Aset Fisik

  Aset Fisik merupakan istilah yang digunakan untuk menggambarkan aset berwujud seperti properti, peralatan, perabot, persediaan dan barang habis pakai.

  Contoh: hardware seperti laptop, AC, server, sensor, genset, UPS, dll.

- Aset Virtual

  Aset virtual adalah segala sumber daya yang dapat memberikan manfaat dan berada di dunia maya serta terkoneksi dengan internet.

  Contoh: software seperti aplikasi operasional, lisensi, cloud, dll.

- Aset Informasi

  Aset informasi adalah sesuatu yang terdefinisi dan terkelola sebagai satu unit informasi sehingga dapat dipahami, dibagi, dilindungi dan dimanfaatkan secara efektif.

  Contoh: Data pribadi, data *source code*, data perjanjian, topologi jaringan, dll.

Pengelolaan Akses

1. Dilaksanakan penetaan akses terhadap setiap aset untuk memastikan tidak ada akses yang tidak sah.
2. Pengelolaan akses yang dilakukan pada poin 1 dimasukkan kedalam form matriks akses
3. Proses pengelolaan hak akses mengacu pada proses:
   - Penyerahan aset dan hak akses pada pegawai baru
   - Permohonan hak akses
   - Perubahan hak akses
   - Penghapusan hak akses
4. Dalam proses poin 3 diperlukan :
   - Form permohonan pembukaan dan penutupan akses

Manajemen Insiden

1. Insiden terbagi menjadi dua yaitu insiden IT (IT dan Kecerdasan IT) dan non IT
2. Setiap laporan insiden dicatat dan diverifikasi oleh Agen Siber
3. Tim menyusun strategi mitigasi terhadap insiden
4. Melaksanakan analisis untuk penanganan insiden siber
5. Tim menyampaikan laporan dan analisis insiden siber ke koordinator
6. Tim dan pihak terkait yang ditunjuk melaksanakan penanganan insiden
7. Pemulihan sistem elektronik yang terdampak
8. Proses selesai

Pengembangan Aplikasi

1. Dalam pengembangan suatu aplikasi, organisasi harus memiliki prinsip-prinsip yang telah ditentukan
2. Organisasi harus memisahkan juga untuk lingkungan pengembangan seperti lingkungan pengembangan, pengujian, dan produksi
3. Organisasi harus memastikan juga apabila suatu aplikasi dikembangkan oleh pihak ketiga, Source Code harus dipegang juga oleh organisasi
4. Setiap perubahan dalam aplikasi perlu didokumentasikan dalam Form Request for Change (RFC)

Monitoring Kapasitas dan Perangkat User

1. Dilakukan pemantauan dan pencatatan kapasitas untuk penyimpanan dan memori di PC setiap bulan.
2. Komponen yang melampaui batas kapasitas harus ditindaklanjuti.
3. Ditentukan batas kapasitas sebagai berikut:
    a. CPU Performance: 90%
    b. Kapasitas Memori: 90%
    c. Kapasitas Disk: 80%
4. Setiap pegawai yang memiliki PC/Laptop harus memantau terkait akses user, *lock screen*, sinkronisasi waktu, antivirus, update OS, scanning dan versi OS
5. Dokumen yang perlu diisi: Form Monitoring Perangkat User dan Form Pemantauan Kapasitas

Matriks Kompetensi

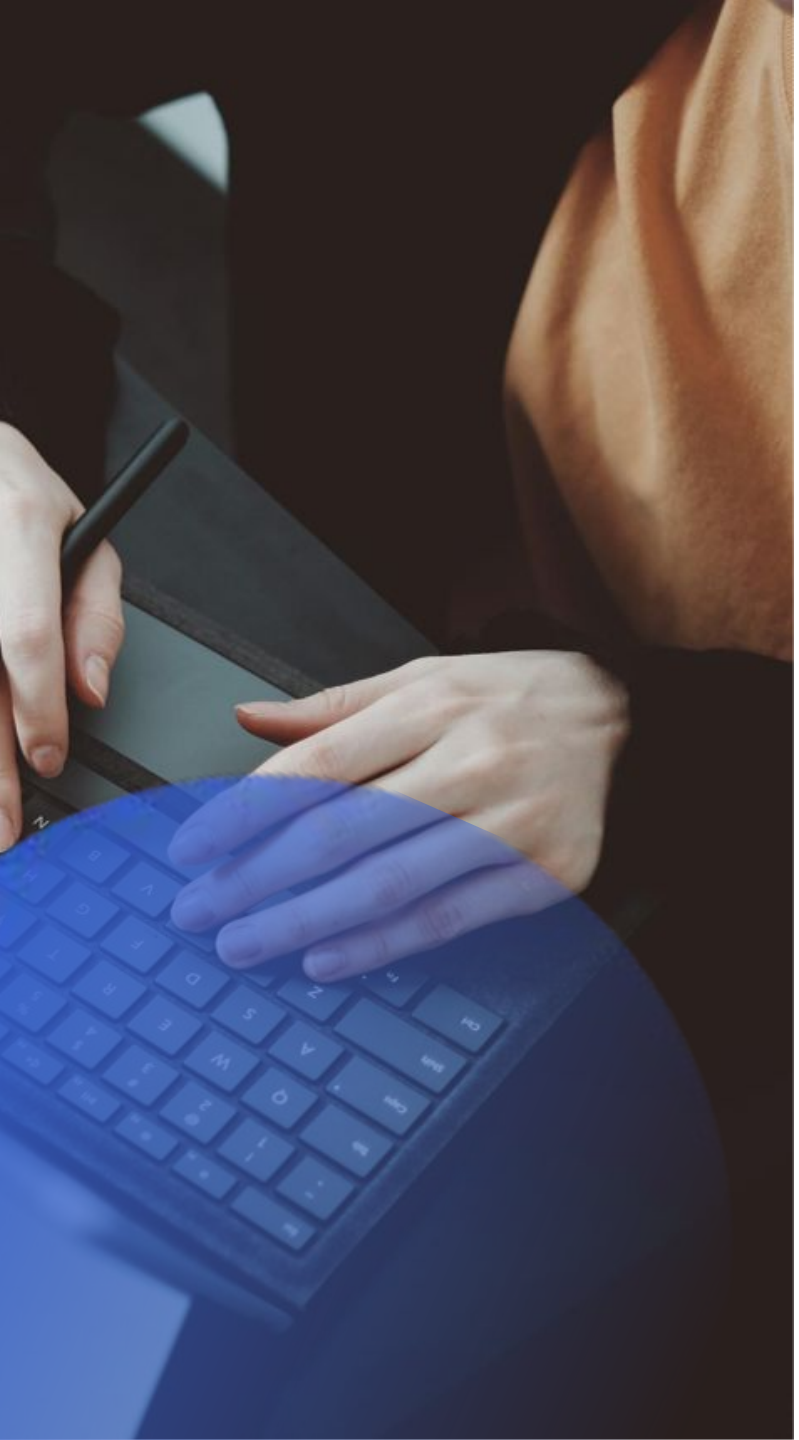
1. Kompetensi yang sudah dimiliki oleh seorang individu berdasarkan pengetahuan, keterampilan, dan pengalaman yang dimiliki saat ini dalam mengelola keamanan informasi (Kompetensi saat ini)
2. Kompetensi yang dibutuhkan oleh seorang individu untuk mendukung kegiatan pengamanan informasi di organisasi (Kompetensi yang dibutuhkan)
3. Kedua jenis kompetensi tersebut dibandingkan dan akan menghasilkan perencanaan pelatihan untuk peningkatan atau pemenuhan kompetensi yang diperlukan.

Kebijakan Meja Bersih

1. Memastikan dokumen rahasia di meja kerja tidak dibiarkan dalam keadaan terbuka jika tidak sedang digunakan
2. Mengunci lemari dan laci yang berisi dokumen rahasia ketika akan meninggalkan ruangan
3. Memastikan untuk segera mengambil dokumen rahasia yang berada di printer, mesin fotokopi, mesin tax, dan memusnahkan dokumen yang tidak terpakai atau salah cetak
4. Tidak menaruh makanan atau minuman diatas meja kerja

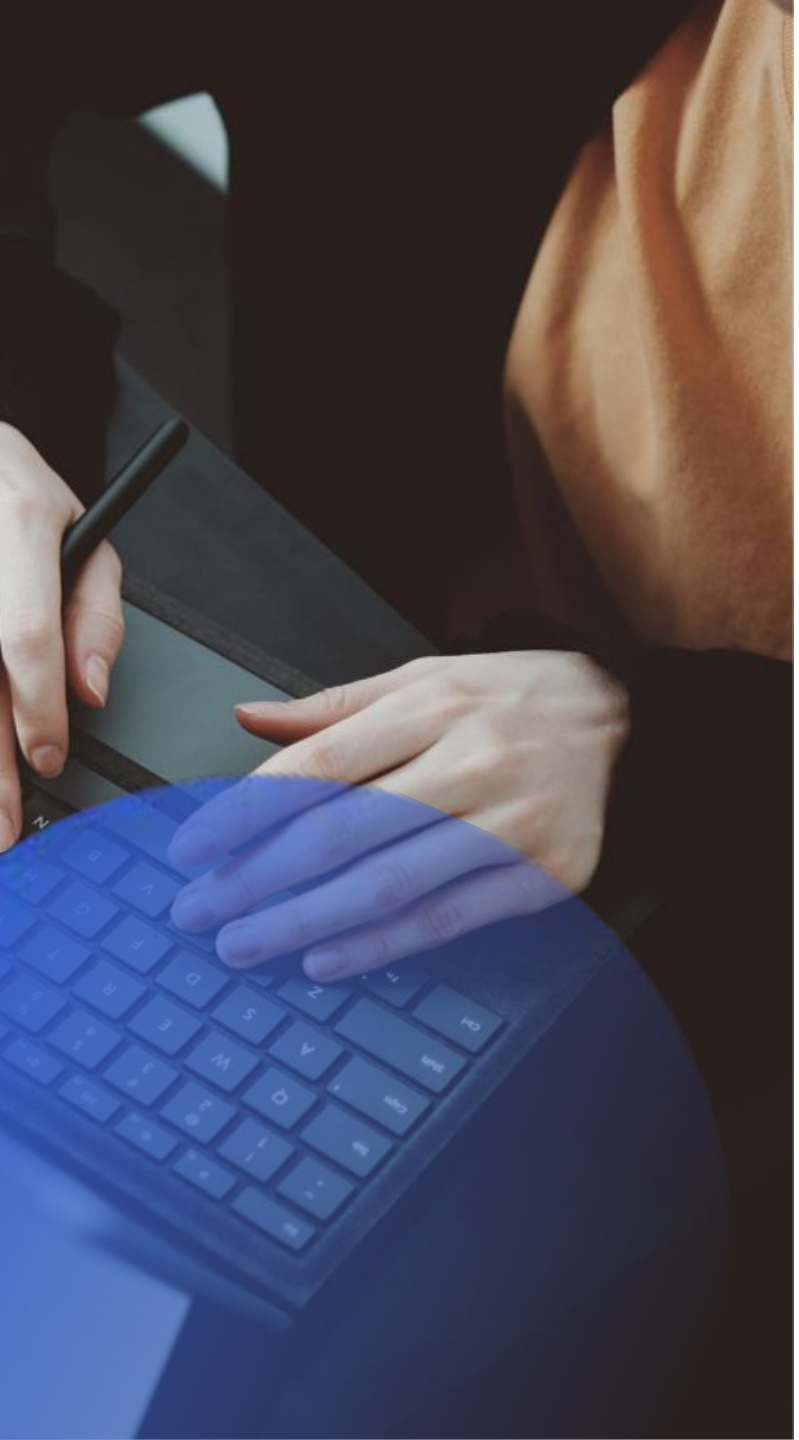
Kebijakan Layar Bersih

1. *Logoff* atau *lock computer* ketika akan meninggalkan *mobile device* dan PC atau ketika ada tamu yang akan datang ke meja kerja.
2. Memastikan informasi rahasia yang tertera di papan tulis/*whiteboard* dan/atau tersimpan (*softcopy*) di papan tulis elektronik/*electronic whiteboard* di ruang rapat dihapus sebelum meninggalkan ruangan.
3. *Autolock* pada masing-masing PC/Laptop yang tidak digunakan selama 10 menit.
4. Password minimum terdiri dari 8 karakter kombinasi angka dan huruf dan simbol serta tidak boleh menggunakan karakter yang mudah ditebak.



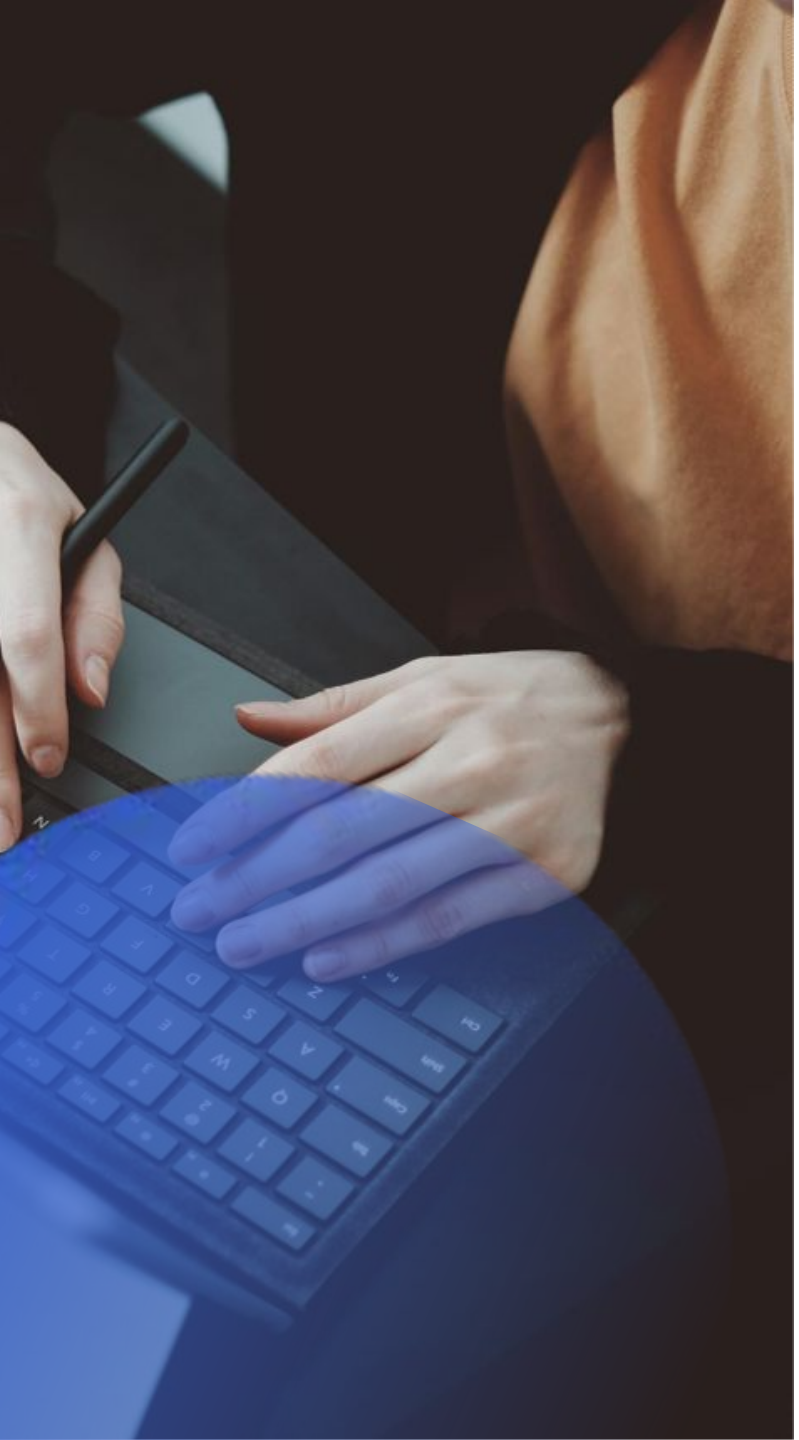
HAL YANG HARUS DILAKUKAN (DO)

- Seluruh pegawai dan pihak eksternal harus mematuhi peraturan di lingkungan Dinas Komunikasi dan Informatika Kabupaten Kudus.
- Memastikan informasi disimpan dengan aman serta segala jenis informasi dan aset memiliki klasifikasi kerahasiaan yang harus dipatuhi.
- Melaporkan dan mendokumentasikan terkait segala jenis kerentanan dan potensi insiden
- Pihak eksternal yang berkaitan dengan Dinas Komunikasi dan Informatika Kabupaten Kudus harus melalui proses uji kelayakan, kemudian menyetujui dan menandatangani syarat dan perjanjian untuk menjaga keamanan informasi dan informasi pribadi di lingkup Dinas Komunikasi dan Informatika Kabupaten Kudus sebelum diberikan akses ke aset Dinas Komunikasi dan Informatika Kabupaten Kudus.
- Memastikan dilakukannya pemeriksaan latar belakang dan uji kelayakan secara menyeluruh baik untuk calon pegawai baru maupun dalam proses seleksi pihak eksternal, sesuai dengan peraturan perundang-undangan yang berlaku.



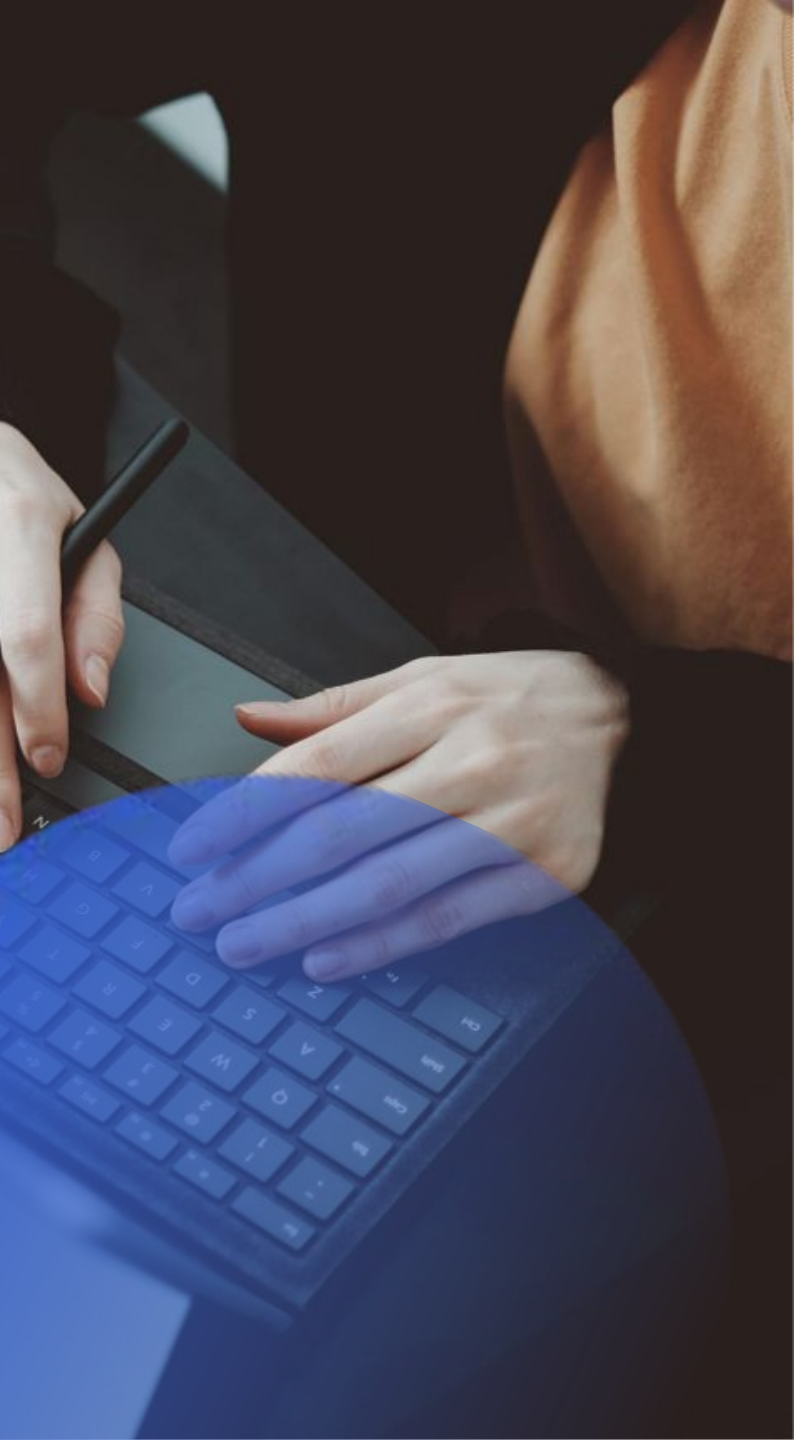
HAL YANG HARUS DILAKUKAN (DO)

- Memastikan seluruh hak akses maupun aset yang dimiliki oleh pegawai dan pihak eksternal harus dicabut apabila yang bersangkutan tidak lagi bekerja di Dinas Komunikasi dan Informatika Kabupaten Kudus.
- Perangkat pengolahan informasi penyimpanan data yang sudah tidak lagi digunakan harus disanitasi sebelum digunakan kembali/dimusnahkan.
- Adanya pembatasan akses terhadap aset kritikal milik Dinas Komunikasi dan Informatika Kabupaten Kudus.
- Menerapkan sistem kriptografi dan penyamaran data (data masking) untuk melindungi informasi di Dinas Komunikasi dan Informatika Kabupaten Kudus.
- Kantor dan ruangan yang berisikan aset informasi kritikal harus dilindungi secara memadai dengan adanya pembatasan zona area kerja.
- Kebijakan meja bersih setelah selesai bekerja harus diterapkan, seperti tidak meninggalkan dokumen fisik di atas meja tanpa pengawasan, menghapus papan tulis, mengaktifkan kunci layar, dan log-off session pada Laptop/PC.



HAL YANG HARUS DILAKUKAN (DO)

- Mematuhi aturan terkait pengembangan perangkat lunak dan sistem di seluruh tahapan siklus pengembangan, seperti melakukan pentest sebelum produksi.
- Mendokumentasikan proses operasional dan pastikan adanya cadangan informasi yang memadai (backup).
- Pastikan kesiapan operasional Dinas Komunikasi dan Informatika Kabupaten Kudus dalam menghadapi ancaman dengan merencanakan simulasi pemulihan bencana.
- Menggunakan enkripsi tambahan untuk melindungi data sensitif pada media removable seperti flashdisk, harddisk yang tidak teregistrasi.
- Menerapkan sistem yang dapat melakukan pendeteksian, pencegahan, dan pemulihan sebagai bentuk perlindungan terhadap ancaman program yang membahayakan (malware).



HAL YANG HARUS DILAKUKAN (DO)

- Patuhi kebijakan keamanan informasi yang berlaku di Dinas Komunikasi dan Informatika Kabupaten Kudus dan perlakukan informasi sebagai aset.
- Lakukan proses penyaringan sumber daya manusia yang memadai dan pastikan adanya perjanjian kerahasiaan dengan pegawai, pemasok, maupun pihak eksternal lainnya *(non-disclosure agreement, NDA)*
- Ikuti prosedur pengendalian akses, patuhi aturan penggunaan akun dan password, serta gunakan enkripsi bilamana diperlukan

Hal yang Harus Dihindari

1. Jangan mengakses informasi terkait pekerjaan di tempat yang tidak aman atau menggunakan jaringan yang tidak terjamin keamanannya.
2. Hindari penggunaan media portable yang tidak teregistrasi seperti USB Flashdisk, hard-disk eksternal, smartphone, tablet, dll.
3. Jangan meninggalkan laptop / workstation tanpa mengunci layar dan jangan meninggalkan dokumen fisik di atas meja tanpa pengawasan
4. Jangan menggunakan perangkat lunak yang tidak berlisensi atau tidak masuk ke dalam *whitelist* organisasi
5. Jangan berbagi akun untuk mengakses informasi
6. Jangan mengubah konfigurasi perangkat, jaringan, dan perangkat lunak tanpa adanya proses manajemen perubahan terlebih dahulu
7. Jangan membiarkan hal-hal yang berpotensi menjadi insiden
8. Jangan membawa aset organisasi keluar organisasi setelah berakhirnya kerja sama dengan organisasi

MITRA BERDAYA OPTIMA

TERIMA KASIH

Contact Us

www.mitraberdaya.id

contact@mitraberdaya.id