MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA

KEPUTUSAN MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA
NOMOR 191 TAHUN 2024
TENTANG
PENETAPAN STANDAR KOMPETENSI KERJA NASIONAL INDONESIA KATEGORI INFORMASI DAN KOMUNIKASI GOLONGAN POKOK AKTIVITAS PEMROGRAMAN, KONSULTASI KOMPUTER DAN KEGIATAN YANG BERHUBUNGAN DENGAN ITU (YBDI) BIDANG KEAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI KETENAGAKERJAAN REPUBLIK INDONESIA,

Menimbang :

a. bahwa untuk memelihara validitas dan reliabilitas Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan Yang Berhubungan Dengan Itu (YBDI) Bidang Keamanan Informasi, perlu dilakukan kaji ulang atas standar kompetensi dimaksud;

b. bahwa berdasarkan hasil kaji ulang sebagaimana dimaksud dalam huruf a telah disepakati Rancangan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan Yang Berhubungan Dengan Itu (YBDI) Bidang Keamanan Informasi melalui konvensi nasional pada tanggal 8 November 2023 di Bali;

c. bahwa sesuai surat Kepala Pusat Penelitian dan Pengembangan Aplikasi Informatika dan Informasi dan Komunikasi Publik Nomor B-726/BLSDM.3/LT.02.02/ 11/2023 tanggal 9 November 2023 perihal Permohonan Penetapan RSKKNI Bidang Keamanan Informasi, perlu ditindaklanjuti dengan menetapkan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktvitas Pemrograman, Konsultasi Komputer dan Kegiatan Yang Berhubungan Dengan Itu (YBDI) Bidang Keamanan Informasi;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Keputusan Menteri Ketenagakerjaan tentang Penetapan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan Yang Berhubungan Dengan Itu (YBDI) Bidang Keamanan Informasi;

Mengingat : 1. Undang-Undang Nomor 13 Tahun 2003 tentang Ketenagakerjaan (Lembaran Negara Republik Indonesia Tahun 2003 Nomor 39, Tambahan Lembaran Negara Republik Indonesia Nomor 4279);
2. Peraturan Pemerintah Nomor 31 Tahun 2006 tentang Sistem Pelatihan Kerja Nasional (Lembaran Negara Republik Indonesia Tahun 2006 Nomor 67, Tambahan Lembaran Negara Republik Indonesia Nomor 4637);
3. Peraturan Presiden Nomor 8 Tahun 2012 tentang Kerangka Kualifikasi Nasional Indonesia (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 24);
4. Peraturan Presiden Nomor 95 Tahun 2020 tentang Kementerian Ketenagakerjaan (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 213);
5. Peraturan Menteri Ketenagakerjaan Nomor 21 Tahun 2014 tentang Pedoman Penerapan Kerangka Kualifikasi Nasional Indonesia (Berita Negara Republik Indonesia Tahun 2014 Nomor 1792);
6. Peraturan Menteri Ketenagakerjaan Nomor 3 Tahun 2016 tentang Tata Cara Penetapan Standar Kompetensi Kerja Nasional Indonesia (Berita Negara Republik Indonesia Tahun 2016 Nomor 258);
7. Peraturan Menteri Ketenagakerjaan Nomor 1 Tahun 2021 tentang Organisasi dan Tata Kerja Kementerian Ketenagakerjaan (Berita Negara Republik Indonesia Tahun 2021 Nomor 108);

MEMUTUSKAN:

Menetapkan : KEPUTUSAN MENTERI KETENAGAKERJAAN TENTANG PENETAPAN STANDAR KOMPETENSI KERJA NASIONAL INDONESIA KATEGORI INFORMASI DAN KOMUNIKASI GOLONGAN POKOK AKTIVITAS PEMROGRAMAN, KONSULTASI KOMPUTER DAN KEGIATAN YANG BERHUBUNGAN DENGAN ITU (YBDI) BIDANG KEAMANAN INFORMASI.

KESATU : Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan Yang Berhubungan Dengan Itu (YBDI) Bidang Keamanan Informasi sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Keputusan Menteri ini.

KEDUA : Standar Kompetensi Kerja Nasional Indonesia sebagaimana dimaksud dalam Diktum KESATU menjadi acuan dalam penyusunan jenjang kualifikasi nasional, penyelenggaraan pendidikan, pelatihan, dan sertifikasi kompetensi.

KETIGA : Pemberlakuan Standar Kompetensi Kerja Nasional Indonesia sebagaimana dimaksud dalam Diktum KESATU dan penyusunan jenjang kualifikasi nasional sebagaimana dimaksud dalam Diktum KEDUA ditetapkan oleh Menteri Komunikasi dan Informatika dan/atau

kementerian/lembaga teknis terkait sesuai dengan tugas dan fungsinya.

KEEMPAT : Standar Kompetensi Kerja Nasional Indonesia sebagaimana dimaksud dalam Diktum KESATU dikaji ulang setiap 5 (lima) tahun atau sesuai dengan kebutuhan.

KELIMA : Penerapan Standar Kompetensi Kerja Nasional Indonesia sebagaimana dimaksud dalam Diktum KESATU berdasarkan Keputusan Menteri Ketenagakerjaan Nomor 55 Tahun 2015 tentang Penetapan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Kegiatan Pemrograman, Konsultasi Komputer dan Kegiatan YBDI Bidang Keamanan Informasi, wajib disesuaikan dengan Keputusan Menteri ini paling lambat 6 (enam) bulan sejak Keputusan Menteri ini berlaku.

KEENAM : Pada saat Keputusan Menteri ini mulai berlaku maka Keputusan Menteri Ketenagakerjaan Nomor 55 Tahun 2015 tentang Penetapan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Kegiatan Pemrograman, Konsultasi Komputer dan Kegiatan YBDI Bidang Keamanan Informasi, dicabut dan dinyatakan tidak berlaku.

KETUJUH : Keputusan Menteri ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 15 Agustus 2024

MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA,

IDA FAUZIYAH

LAMPIRAN
KEPUTUSAN MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA
NOMOR 191 TAHUN 2024
TENTANG
PENETAPAN STANDAR KOMPETENSI KERJA KATEGORI INFORMASI DAN KOMUNIKASI GOLONGAN POKOK AKTIVITAS PEMROGRAMAN, KONSULTASI KOMPUTER DAN KEGIATAN YANG BERHUBUNGAN DENGAN ITU (YBDI) BIDANG KEAMANAN INFORMASI

BAB I
PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi yang pesat di Indonesia, seperti peningkatan akses internet, adopsi teknologi komputasi awan, kecerdasan buatan, *big data*, dan transformasi digital, menciptakan lingkungan kompleks dalam domain keamanan informasi. Banyaknya data dan informasi strategis, serta data pribadi yang dihasilkan oleh suatu organisasi maupun individu melalui teknologi-teknologi tersebut, berpotensi membawa risiko keamanan seperti pencurian data, serangan *malware*, dan ancaman lainnya. Adanya risiko keamanan tersebut dapat menimbulkan pelanggaran hukum, kerugian finansial bahkan merusak reputasi organisasi atau pribadi seseorang. Hal ini menunjukkan pentingnya penerapan kebijakan dan praktik keamanan informasi yang efektif untuk melindungi informasi dari risiko yang timbul.

Dalam rangka menerapkan kebijakan dan praktik keamanan informasi tersebut, para profesional di bidang keamanan informasi memiliki peran yang sangat penting. Mereka merupakan garda terdepan yang bertanggung jawab atas keamanan sistem, jaringan, dan informasi sensitif. Di sisi lain, dalam menghadapi ancaman yang terus berkembang, mereka harus selalu siap untuk mengikuti perkembangan teknologi maupun metode serangan baru. Oleh karena itu kemampuan para profesional tersebut juga dituntut untuk terus berkembang melalui pendidikan formal maupun informal di bidang keamanan informasi. Sehubungan dengan hal tersebut, maka dibutuhkan standar kompetensi di bidang keamanan informasi sebagai acuan kualifikasi kompetensi kerja sesuai dengan kebutuhan para pemangku kepentingan guna menjamin ketersediaan tenaga kerja yang profesional di bidang keamanan informasi.

Kompetensi kerja di bidang keamanan informasi dapat diukur berdasarkan pengetahuan, keterampilan dan sikap yang dimiliki oleh seseorang profesional yang dituangkan ke dalam Standar Kompetensi Kerja Nasional Indonesia (SKKNI). SKKNI merupakan panduan yang berisi pengetahuan dan keterampilan yang diharapkan dimiliki oleh para profesional di bidang keamanan informasi. Menteri Ketenagakerjaan dengan Keputusan Nomor 55 Tahun 2015 telah menetapkan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan Yang Berhubungan Dengan Itu (YBDI) Bidang keamanan informasi. Namun demikian, dalam menghadapi ancaman yang semakin kompleks, SKKNI Bidang keamanan informasi ini perlu diperbarui secara berkala agar tetap relevan dan efektif. Melalui kaji ulang tersebut

diharapkan SKKNI Bidang keamanan informasi menjadi lebih selaras dengan kebutuhan keamanan informasi pada setiap lapisan organisasi, sektor dan masyarakat. Selain itu, SKKNI yang telah dikaji ulang nanti akan mampu menjawab perkembangan teknologi, perubahan regulasi dan kebijakan, serta lebih terukur, tertelusur, terdeskripsi secara jelas dan lengkap. Dengan adanya SKKNI Bidang keamanan informasi hasil kaji ulang diharapkan menjadi lebih mudah untuk dipakai sebagai acuan dalam pendidikan, penyusunan program pelatihan berbasis kompetensi serta penyusunan skema sertifikasi dan penyusunan materi uji kompetensi.

Sesuai dengan perkembangan pemanfaatan teknologi dan kebutuhan keamanan informasi pada saat ini, maka fungsi kunci yang ditetapkan pada peta kompetensi SKKNI Bidang keamanan informasi adalah menerapkan prinsip dasar keamanan informasi dan pengendalian sumber daya keamanan informasi. Prinsip dasar keamanan informasi adalah seperangkat aturan dan pedoman yang dirancang untuk melindungi informasi pada aspek Kerahasiaan, Integritas, dan ketersediaan informasi termasuk aspek keamanan yang melekat lainnya seperti Autentikasi, otorisasi dan non-repudiasi. Di sisi lain, pengendalian sumber daya keamanan informasi merujuk pada langkah-langkah yang diambil untuk memastikan bahwa sumber daya yang terkait dengan keamanan informasi, seperti perangkat keras, perangkat lunak, jaringan, dan personel serta lingkungan fisik, dikelola dan dimanfaatkan secara efektif guna melindungi informasi yang sensitif dan penting.

B. Pengertian

1. Aset Teknologi Informasi atau Aset TI meliputi informasi, perangkat keras, perangkat lunak dan sumber daya manusia yang bernilai dan bermanfaat untuk mencapai tujuan perusahaan/organisasi. Aset perangkat keras dapat mencakup *workstation* dan komponennya, perangkat jaringan, *printer*, *smartphone*, dan lain-lain. Aset perangkat lunak dapat mencakup lisensi, instalasi, *Operating System* (OS), dan lain-lain.
2. Autentikasi adalah sifat atau keadaan informasi yang dapat dikonfirmasi pengirimnya atau keasliannya.
3. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *Electronic Data Interchange* (EDI), surat elektronik (*electronic mail*, telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
4. Integritas adalah sifat atau keadaan informasi yang melindungi keakuratan dan kelengkapan aset serta memastikan aset hanya dapat dimodifikasi oleh pihak yang berwenang.
5. Keamanan Informasi adalah pelindungan informasi dan sistem informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran yang tidak sah untuk menjaga Kerahasiaan, Integritas, dan Ketersediaan.
6. Kebutuhan Keamanan Informasi mencakup berbagai aspek untuk melindungi Kerahasiaan, Integritas, dan Ketersediaan informasi. Beberapa Kebutuhan Keamanan Informasi yang umum meliputi: keamanan Kerahasiaan, keamanan Integritas, keamanan Ketersediaan, keaslian identitas, keamanan jaringan, manajemen akses, pelacakan dan audit dan kesadaran keamanan.

7. Kerahasiaan adalah sifat atau keadaan informasi yang tidak disediakan atau dibuka untuk perorangan, lembaga atau proses yang tidak berwenang.
8. Ketersediaan adalah sifat atau keadaan informasi yang dapat diakses dan digunakan sesuai permintaan lembaga yang berwenang.

C. Penggunaan SKKNI

Standar Kompetensi dibutuhkan oleh beberapa lembaga/institusi yang berkaitan dengan pengembangan sumber daya manusia, sesuai dengan kebutuhan masing-masing:

1. Untuk institusi pendidikan dan pelatihan
   a. Memberikan informasi untuk pengembangan program dan kurikulum.
   b. Sebagai acuan dalam penyelenggaraan pelatihan, penilaian, dan sertifikasi.
2. Untuk dunia usaha/industri dan penggunaan tenaga kerja
   a. Membantu dalam rekrutmen.
   b. Membantu penilaian unjuk kerja.
   c. Membantu dalam menyusun uraian jabatan.
   d. Membantu dalam mengembangkan program pelatihan yang spesifik berdasar kebutuhan dunia usaha/industri.
3. Untuk institusi penyelenggara pengujian dan sertifikasi
   a. Sebagai acuan dalam merumuskan paket-paket program sertifikasi sesuai dengan kualifikasi dan levelnya.
   b. Sebagai acuan dalam penyelenggaraan pelatihan penilaian dan sertifikasi.

D. Komite Standar Kompetensi

Susunan komite standar kompetensi pada Standar Kompetensi Kerja Nasional Indonesia (SKKNI) Bidang Keamanan Informasi dibentuk melalui Keputusan Kepala Badan Penelitian dan Pengembangan Sumber Daya Manusia Kementerian Komunikasi dan Informatika Nomor 33 tanggal 27 Februari 2023 dapat dilihat pada Tabel 1 serta susunan Tim Perumus dan Tim Verifikasi dapat dilihat pada Tabel 2 dan Tabel 3.

Tabel 1. Susunan Komite Standar Kompetensi SKKNI Bidang Keamanan Informasi

NO.	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Kepala Badan Penelitian dan Pengembangan Sumber Daya Manusia	Kementerian Komunikasi dan Informatika	Pengarah
2.	Kepala Puslitbang Aplikasi Informatika dan Informasi dan Komunikasi Publik	Kementerian Komunikasi dan Informatika	Ketua
3.	Sekretaris Badan Penelitian dan Pengembangan Sumber Daya Manusia	Kementerian Komunikasi dan Informatika	Sekretaris
4.	Direktur Tata Kelola Aplikasi Informatika	Kementerian Komunikasi dan Informatika	Anggota

NO.	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
5.	Kepala Biro Perencanaan	Kementerian Komunikasi dan Informatika	Anggota
6.	Sekretaris Direktorat Jenderal Aplikasi dan Informatika	Kementerian Komunikasi dan Informatika	Anggota
7.	Sekretaris Direktorat Jenderal Informasi dan Komunikasi Publik	Kementerian Komunikasi dan Informatika	Anggota
8.	Sekretaris Direktorat Jenderal Penyelenggaraan Pos dan Informatika	Kementerian Komunikasi dan Informatika	Anggota
9.	Sekretaris Direktorat Jenderal Sumber Daya Perangkat Pos dan Informatika	Kementerian Komunikasi dan Informatika	Anggota
10.	Ketua Indonesia Cyber Security Forum	Indonesia Cyber Security Forum	Anggota
11.	Ketua Umum Ikatan Profesi Komputer dan Informatika Indonesia	Ikatan Profesi Komputer dan Informatika Indonesia	Anggota
12.	Ketua Umum Ikatan Ahli Informatika Indonesia	Ikatan Ahli Informatika Indonesia	Anggota
13.	Ketua Umum Asosiasi Piranti Lunak Telematika Indonesia	Asosiasi Piranti Lunak Telematika Indonesia	Anggota
14.	Ketua Umum Asosiasi Profesi Fotografi Indonesia	Asosiasi Profesi Fotografi Indonesia	Anggota
15.	Ketua Umum Asosiasi Game Indonesia	Asosiasi Game Indonesia	Anggota
16.	Ketua Umum Ikatan Audit Sistem Informasi Indonesia	Ikatan Audit Sistem Informasi Indonesia	Anggota
17.	Direktur Kebijakan SDM Keamanan Siber dan Sandi BSSN	Badan Siber dan Sandi Negara	Anggota

Tabel 2. Susunan Tim Perumus SKKNI Bidang Keamanan Informasi

NO.	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Anton Setiyawan	PT PCI Profesi Indonesia	Ketua
2.	I Made Wiryana	Universitas Gunadarma	Sekretaris
3.	Enggar Ndaru Prasojo	Badan Siber dan Sandi Negara	Anggota
4.	Eko Yon Handri	Badan Siber dan Sandi Negara	Anggota

NO.	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
5.	Santi Indarjani	Politeknik Siber dan Sandi Negara	Anggota
6.	Satriyo Wibowo	ICSF dan PT Xynexis Indonesia	Anggota
7.	Didik Partono	Inixindo/ASPILUKI/ IPKIN	Anggota
8.	Siswanto	Universitas Budi Luhur/Ikatan Ahli Informatika Indonesia (IAII)	Anggota
9.	Lucia Istyowati	Institute Perbanas Jakarta	Anggota
10.	Bety Hayat Susanti	Politeknik Siber dan Sandi Negara	Anggota
11.	Menhariq Noor	Direktorat Tata Kelola Aplikasi Informatika, Kementerian Komunikasi dan Informatika	Anggota

Tabel 3. Susunan Tim Verifikasi SKKNI Bidang Keamanan Informasi

NO.	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Cut Medika Z	Kementerian Komunikasi dan Informatika	Ketua
2.	Aldhino Anggorosesar	Kementerian Komunikasi dan Informatika	Anggota
3.	Yan Andriariza	Kementerian Komunikasi dan Informatika	Anggota
4.	Lidya Agustina	Kementerian Komunikasi dan Informatika	Anggota
5.	Annisa Muthia Yana	Kementerian Komunikasi dan Informatika	Anggota
6.	Olivia Nelar	Kementerian Komunikasi dan Informatika	Anggota
7.	Anas Hilal	Badan Siber dan Sandi Negara	Anggota
8.	Roybafih Sukisman	Badan Siber dan Sandi Negara	Anggota
9.	Wuri Handayani	Badan Siber dan Sandi Negara	Anggota
10.	Muhammad Lutfi	Badan Siber dan Sandi Negara	Anggota

BAB II
STANDAR KOMPETENSI KERJA NASIONAL INDONESIA

A. Pemetaan Standar Kompetensi

TUJUAN UTAMA	FUNGSI KUNCI	FUNGSI UTAMA	FUNGSI DASAR
Mengelola sistem informasi yang aman dan akuntabel berdasarkan aturan dan kebijakan yang berlaku	Menerapkan prinsip dasar Keamanan Informasi	Mengimplemen-tasikan prinsip Kerahasiaan informasi	Mengklasifikasikan informasi yang bersifat rahasia
			Melaksanakan pengamanan informasi yang bersifat rahasia
		Memastikan Integritas dalam melindungi informasi dari perubahan, perusakan dan penyalahgunaan	Melaksanakan pengamanan Integritas informasi
			Melaksanakan validasi Integritas informasi
		Memastikan Ketersediaan informasi organisasi dan aset terkait	Melaksanakan keberlangsungan Keamanan Informasi
			Mengimplementa-sikan penyediaan fasilitas pemrosesan informasi dengan redundansi yang sesuai
		Memastikan Autentikasi informasi dan komunikasi berasal dari sumber yang tepercaya	Menetapkan metode Autentikasi
			Melaksanakan Autentikasi dalam upaya mencegah peniruan identitas
			Melaksanakan Autentikasi dalam upaya mencegah pemalsuan informasi
		Melaksanakan pengendalian akses Aset Teknologi Informasi	Menentukan Aset Teknologi Informasi yang dikontrol
			Melaksanakan pengontrolan akses pengguna yang berwenang

	Menerapkan pengendalian sumber daya Keamanan Informasi	Mengimple-mentasikan pengendalian fisik Keamanan Informasi	Menentukan metode pelindungan fisik Keamanan Informasi
			Menyusun rencana pelaksanaan pelindungan fisik Keamanan Informasi
		Mengimplemen-tasikan pengendalian personel Keamanan Informasi	Memetakan profil sumber daya manusia Keamanan Informasi
			Menyusun dokumen skrining personel Keamanan Informasi
		Mengimplemen-tasikan pengendalian teknologi Keamanan Informasi	Menerapkan teknologi Keamanan Informasi sesuai dengan ketentuan yang berlaku
			Menyusun rencana penerapan aspek Keamanan Informasi pada pemutakhiran teknologi informasi
		Mengimplemen-tasikan pengendalian kebijakan Keamanan Informasi	Menyusun rencana penerapan kebijakan Keamanan Informasi
			Melaksanakan pemantauan penerapan kebijakan Keamanan Informasi

B. Daftar Unit Kompetensi

NO.	KODE UNIT	JUDUL UNIT KOMPETENSI
1	*2*	*3*
1.	J.62KAM00.001.2	Mengklasifikasikan Informasi yang Bersifat Rahasia
2.	J.62KAM00.002.1	Melaksanakan Pengamanan Informasi yang Bersifat Rahasia
3.	J.62KAM00.003.2	Melaksanakan Pengamanan Integritas Informasi
4.	J.62KAM00.004.2	Melaksanakan Validasi Integritas Informasi
5.	J.62KAM00.005.1	Melaksanakan Keberlangsungan Keamanan Informasi
6.	J.62KAM00.006.2	Mengimplementasikan Penyediaan Fasilitas Pemrosesan Informasi dengan Redundansi yang sesuai
7.	J.62KAM00.007.1	Menetapkan Metode Autentikasi
8.	J.62KAM00.008.1	Melaksanakan Autentikasi dalam Upaya Mencegah Peniruan Identitas
9.	J.62KAM00.009.1	Melaksanakan Autentikasi dalam Upaya Mencegah Pemalsuan Informasi
10.	J.62KAM00.010.1	Menentukan Aset Teknologi Informasi yang Dikontrol
11.	J.62KAM00.011.2	Melaksanakan Pengontrolan Akses Pengguna yang Berwenang
12.	J.62KAM00.012.2	Menentukan Metode Pelindungan Fisik Keamanan Informasi
13.	J.62KAM00.013.2	Menyusun Rencana Pelaksanaan Pelindungan Fisik Keamanan Informasi
14.	J.62KAM00.014.2	Memetakan Profil Sumber Daya Manusia Keamanan Informasi
15.	J.62KAM00.015.1	Menyusun Dokumen Skrining Personel Keamanan Informasi
16.	J.62KAM00.016.1	Menerapkan Teknologi Keamanan Informasi sesuai dengan Ketentuan yang Berlaku
17.	J.62KAM00.017.2	Menyusun Rencana Penerapan Aspek Keamanan Informasi pada Pemutakhiran Teknologi Informasi
18.	J.62KAM00.018.2	Menyusun Rencana Penerapan Kebijakan Keamanan Informasi
19.	J.62KAM00.019.2	Melaksanakan Pemantauan Penerapan Kebijakan Keamanan Informasi

C. Uraian Unit Kompetensi

KODE UNIT : **J.62KAM00.001.2**
JUDUL UNIT : **Mengklasifikasikan Informasi yang Bersifat Rahasia**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengklasifikasikan informasi yang bersifat rahasia melalui pembuatan kategori klasifikasi informasi dan penentuan informasi yang bersifat rahasia.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Membuat kategori klasifikasi informasi	1.1 **Kategori klasifikasi informasi** diidentifikasi berdasarkan Kebutuhan Keamanan Informasi. 1.2 Hasil identifikasi kategori klasifikasi informasi dianalisis sesuai Kebutuhan Keamanan Informasi. 1.3 Kategori klasifikasi informasi disusun berdasarkan hasil analisis.
2. Mendata informasi yang bersifat rahasia	2.1 **Daftar informasi** diinventarisasi sesuai kategori klasifikasi informasi. 2.2 Daftar informasi yang bersifat rahasia disusun sesuai **format yang berlaku** di organisasi.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk membuat kategori klasifikasi informasi dan menentukan informasi yang bersifat rahasia.
   1.2 Kategori klasifikasi informasi merupakan pengkategorian/penggolongan informasi berdasarkan pada tingkat keseriusan dampak yang ditimbulkan terhadap kepentingan dan keamanan negara, publik, dan perorangan. Kategori klasifikasi dapat merujuk berdasarkan standar antara lain:
      a. SNI ISO/IEC 27001 Keamanan Informasi, keamanan siber, dan proteksi privasi-Sistem manajemen Keamanan Informasi–Persyaratan.
      b. SNI ISO/IEC 27002 Keamanan Informasi, keamanan siber, dan proteksi privasi – Kontrol Keamanan Informasi, NIST SP 800-53 *Security and Privacy Controls for Information Systems and Organizations, Center for Internet Security-Critical Security Controls* (*CIS – CSC*).
      c. Standar yang berlaku lainnya.
   1.3 Daftar informasi merupakan catatan yang berisi keterangan secara sistematis tentang seluruh informasi yang ada di organisasi.
   1.4 Format yang berlaku merupakan standar atau aturan dalam hal tata letak, struktur, dan penulisan dokumen yang konsisten dan sesuai dengan kebijakan dan pedoman yang ditetapkan oleh organisasi.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer atau perangkat pengolah data
      2.1.2 Internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
       (Tidak ada.)
   4.2 Standar
       (Tidak ada.)

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
       3.1.1 Klasifikasi informasi
       3.1.2 Identifikasi risiko Keamanan Informasi
   3.2 Keterampilan
       3.2.1 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami dalam menjabarkan klasifikasi informasi dan daftar informasi yang bersifat rahasia

4. Sikap kerja yang diperlukan
   4.1 Objektif dalam membuat kategori dan menentukan klasifikasi informasi yang bersifat rahasia
   4.2 Teliti dalam membuat kategori dan menentukan klasifikasi informasi yang bersifat rahasia

5. Aspek kritis
   5.1 Ketepatan dalam mengidentifikasi kategori klasifikasi informasi berdasarkan Kebutuhan Keamanan Informasi

KODE UNIT : **J.62KAM00.002.1**
JUDUL UNIT : **Melaksanakan Pengamanan Informasi yang Bersifat Rahasia**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melaksanakan pengamanan informasi yang bersifat rahasia melalui penentuan kebijakan kriptografi sesuai kategori klasifikasi informasi dan penentuan metode enkripsi data.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menentukan kebijakan kriptografi	1.1 **Kebijakan kriptografi** diidentifikasi sesuai Kebutuhan Keamanan Informasi. 1.2 Kebijakan kriptografi dipilih sesuai **kategori klasifikasi informasi.**
2. Menentukan metode enkripsi data	2.1 **Metode enkripsi** diidentifikasi berdasarkan kebijakan kriptografi. 2.2 Metode enkripsi dipilih berdasarkan kebijakan kriptografi.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk menentukan kebijakan kriptografi dan menentukan metode enkripsi data yang sesuai dengan standar.
   1.2 Kebijakan kriptografi merupakan rangkaian konsep dan asas yang menjadi garis besar dan dasar rencana dalam penerapan berbagai prinsip, sarana dan metode untuk transformasi data dalam rangka menyembunyikan kandungan semantik, mencegah penyalahgunaan wewenang, atau mencegah modifikasi tak terdeteksi.
   1.3 Kategori klasifikasi informasi merupakan pengkategorian/penggolongan informasi berdasarkan pada tingkat keseriusan dampak yang ditimbulkan terhadap kepentingan dan keamanan negara, publik dan perorangan. Kategori klasifikasi dapat merujuk standar antara lain:
      a. SNI ISO/IEC 27001 Keamanan Informasi, keamanan siber, dan proteksi privasi – Sistem manajemen Keamanan Informasi – Persyaratan, SNI ISO/IEC 27002 Keamanan Informasi, keamanan siber, dan proteksi privasi – Kontrol Keamanan Informasi.
      b. NIST SP 800-53 *Security and Privacy Controls for Information Systems and Organizations, Center for Internet Security – Critical Security Controls (CIS – CSC).*
      c. Standar yang berlaku lainnya.
   1.4 Metode enkripsi merupakan metode yang mengubah data menjadi kode yang tidak dapat dibaca atau diakses oleh pihak yang tidak sah, antara lain metode enkripsi simetris, metode enkripsi asimetris, dan fungsi *hash*.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer atau perangkat pengolah data
      2.1.2 Internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
   4.2.1 SNI ISO/IEC 27001 Keamanan Informasi, keamanan siber, dan proteksi privasi – Sistem manajemen Keamanan Informasi – Persyaratan

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
   3.1.1 Metode enkripsi
   3.1.2 Prinsip-prinsip Keamanan Informasi
   3.2 Keterampilan
   3.2.1 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami dalam menjabarkan kebijakan kriptografi dan metode enkripsi yang dipilih

4. Sikap kerja yang diperlukan
   4.1 Objektif dalam menentukan kebijakan kriptografi dan metode enkripsi data yang sesuai
   4.2 Teliti dalam menentukan kebijakan kriptografi dan metode enkripsi data yang sesuai
   4.3 Berpikir sistematis dalam menentukan kebijakan kriptografi dan metode enkripsi data yang sesuai

5. Aspek kritis
   5.1 Ketepatan dalam memilih metode enkripsi berdasarkan kebijakan kriptografi

KODE UNIT : **J.62KAM00.003.2**
JUDUL UNIT : **Melaksanakan Pengamanan Integritas Informasi**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menentukan tingkat kepentingan informasi dan metode pengamanan Integritas informasi yang dibutuhkan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menentukan tingkat kepentingan informasi	1.1 **Tingkat kepentingan informasi** diidentifikasi berdasarkan Kebutuhan Keamanan Informasi. 1.2 Hasil identifikasi tingkat kepentingan informasi dianalisis sesuai Kebutuhan Keamanan Informasi. 1.3 Daftar tingkat kepentingan informasi disusun berdasarkan hasil analisis.
2. Menentukan metode pengamanan Integritas informasi	2.1 **Metode pengamanan Integritas informasi** diidentifikasi sesuai dengan tingkat kepentingan informasi. 2.2 Metode pengamanan Integritas informasi dipilih sesuai dengan tingkat kepentingan informasi.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk menjaga keaslian, keakuratan, dan kelengkapan informasi yang penting bagi organisasi.
   1.2 Tingkat kepentingan informasi merupakan ukuran atau nilai yang diberikan pada suatu informasi baik yang bersifat rahasia maupun terbuka berdasarkan kebutuhan pelindungan informasi bagi individu, organisasi, atau sistem. Tingkat kepentingan informasi dapat bervariasi tergantung pada konteks dan kebutuhan pengguna informasi tersebut, sebagai contoh informasi peringatan dini bencana dari badan/organisasi yang berwenang memiliki tingkat kepentingan lebih tinggi dibandingkan informasi jadwal kegiatan *workshop*. Secara umum dapat disesuaikan dengan kebutuhan pengguna, urutan tingkat kepentingan informasi adalah sangat penting, penting, dan biasa.
   1.3 Metode pengamanan Integritas informasi merupakan cara yang digunakan untuk menjaga Integritas informasi dari upaya manipulasi informasi yang merugikan. Salah satu metode pengamanan Integritas informasi adalah penggunaan nilai *hash* dan tanda tangan digital.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer atau perangkat pengolahan data
      2.1.2 Aplikasi pengamanan Integritas informasi
      2.1.3 Internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
      4.2.1 SNI ISO/IEC 27001 Keamanan Informasi, keamanan siber, dan proteksi privasi – Sistem manajemen Keamanan Informasi – Persyaratan

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Teknik kriptografi
   3.2 Keterampilan
      3.2.1 Menggunakan aplikasi pengolah data
      3.2.2 Menggunakan aplikasi pengamanan Integritas informasi

4. Sikap kerja yang diperlukan
   4.1 Teliti dalam mengidentifikasi tingkat kepentingan informasi
   4.2 Sistematis dalam melaksanakan langkah-langkah pengamanan sesuai metode pengamanan Integritas informasi
   4.3 Adaptif terhadap perubahan tingkat kepentingan informasi dan metode pengamanan Integritas informasi

5. Aspek kritis
   5.1 Ketepatan dalam mengidentifikasi metode pengamanan Integritas informasi yang sesuai dengan tingkat kepentingan informasi

KODE UNIT : **J.62KAM00.004.2**
JUDUL UNIT : **Melaksanakan Validasi Integritas Informasi**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengidentifikasi ancaman, metode validasi dan mendokumentasikan hasil validasi Integritas informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi ancaman terhadap Integritas informasi	1.1 **Informasi terkait ancaman Integritas informasi** diinventarisasi berdasarkan Kebutuhan Keamanan Informasi. 1.2 Hasil inventarisasi ancaman Integritas informasi dipilih berdasarkan Kebutuhan Keamanan Informasi.
2. Mengidentifikasi metode validasi Integritas informasi	2.1 **Metode validasi Integritas informasi** diinventarisasi berdasarkan ancaman. 2.2 Metode validasi Integritas informasi ditentukan berdasarkan praktik terbaik Keamanan Informasi.
3. Mendokumentasikan hasil validasi Integritas informasi	3.1 Integritas informasi divalidasi berdasarkan metode validasi. 3.2 Hasil validasi Integritas informasi dicatat berdasarkan Kebutuhan Keamanan Informasi.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk memastikan bahwa informasi yang tersimpan atau dikirimkan tetap utuh dan tidak mengalami perubahan yang tidak sah atau tidak diinginkan.
   1.2 Informasi terkait ancaman Integritas informasi merupakan segala sesuatu yang berpotensi menyebabkan gangguan terhadap Integritas informasi sehingga mengalami kerusakan dan perubahan informasi tersebut.
   1.3 Metode validasi Integritas informasi merupakan cara untuk memastikan bahwa informasi tetap utuh dan tidak mengalami perubahan yang tidak sah atau tidak diinginkan dengan menggunakan metode kriptografi tertentu.

2. Peralatan dan perlengkapan yang diperlukan
   2.1 Peralatan
      2.1.1 Komputer atau perangkat pengolahan data
      2.1.2 Aplikasi pengamanan Integritas informasi
      2.1.3 Internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)

4.2 Standar
4.2.1 SNI ISO/IEC 27001 Keamanan Informasi, keamanan siber, dan proteksi privasi – Sistem manajemen Keamanan Informasi – Persyaratan

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Teknik kriptografi
      3.1.2 Risiko dan ancaman Keamanan Informasi
      3.1.3 Metode validasi Integritas informasi
   3.2 Keterampilan
      3.2.1 Menggunakan aplikasi pengolah data
      3.2.2 Menggunakan aplikasi validasi Integritas informasi

4. Sikap kerja yang diperlukan
   4.1 Teliti dalam memvalidasi Integritas informasi
   4.2 Sistematis dalam melaksanakan langkah-langkah validasi sesuai metode pengamanan Integritas informasi
   4.3 Adaptif terhadap perubahan risiko dan metode pengamanan Integritas informasi

5. Aspek kritis
   5.1 Ketepatan dalam menentukan metode validasi Integritas informasi berdasarkan praktik terbaik Keamanan Informasi

KODE UNIT : **J.62KAM00.005.1**
JUDUL UNIT : **Melaksanakan Keberlangsungan Keamanan Informasi**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melaksanakan keberlangsungan Keamanan Informasi melalui penyusunan rencana kesiapan Teknologi Informasi dan Komunikasi (TIK) untuk keberlangsungan bisnis dan pengamanan Ketersediaan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menyusun daftar kesiapan TIK untuk keberlangsungan bisnis	1.1 Aset Teknologi Informasi (Aset TI) diinventarisasi berdasarkan **proses bisnis organisasi.** 1.2 **Daftar kesiapan TIK** untuk keberlangsungan bisnis dibuat berdasarkan proses bisnis organisasi. 1.3 Daftar kesiapan TIK ditinjau berdasarkan proses bisnis organisasi.
2. Melakukan pengamanan Ketersediaan	2.1 Prosedur operasional pencadangan informasi ditentukan sesuai dengan **disrupsi** yang terjadi. 2.2 Prosedur identifikasi insiden Keamanan Informasi ditentukan sesuai dengan disrupsi yang terjadi. 2.3 Prosedur **restorasi** ditentukan sesuai dengan disrupsi yang terjadi.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk menyusun rencana kesiapan TIK untuk kesiapan bisnis dan melakukan pengamanan Ketersediaan.
   1.2 Proses bisnis organisasi merujuk pada serangkaian langkah atau aktivitas yang dilakukan untuk mencapai tujuan organisasi terkait Keamanan Informasi.
   1.3 Daftar kesiapan TIK merupakan dokumen organisasi yang berisi daftar Aset TI yang digunakan dalam proses bisnis organisasi meliputi untuk layanan, pengolahan, penyimpanan dan sebagainya.
   1.4 Disrupsi merupakan gangguan yang menyebabkan tidak tersedianya produk dan layanan yang diharapkan sesuai dengan sasaran organisasi, disrupsi dapat berupa gangguan yang terantisipasi maupun yang tidak terantisipasi.
   1.5 Restorasi merupakan pengembalian atau pemulihan produk dan layanan ke keadaan semula.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer atau perangkat pengolahan data
      2.1.2 Internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
      4.2.1 SNI ISO/IEC 27001 Keamanan Informasi, keamanan siber, dan proteksi privasi – Sistem manajemen Keamanan Informasi – Persyaratan
      4.2.2 SNI ISO/IEC 27002 Keamanan Informasi, keamanan siber, dan proteksi privasi – Kontrol Keamanan Informasi
      4.2.3 NIST *Special Publication* (SP) 800-34, *Revision* 1, *Contingency Planning Guide for Federal Information Systems*

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Identifikasi Aset TI
      3.1.2 Pemahaman terkait proses bisnis organisasi
   3.2 Keterampilan
      3.2.1 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami dalam menjabarkan rencana kesiapan TIK dalam mendukung organisasi

4. Sikap kerja yang diperlukan
   4.1 Teliti dalam menginventarisasi Aset TI berdasarkan proses bisnis organisasi
   4.2 Berpikir sistematis dalam menentukan prosedur operasional pencadangan
   4.3 Objektif dalam meninjau rencana kesiapan TIK

5. Aspek kritis
   5.1 Ketepatan dalam membuat rencana kesiapan TIK untuk kesiapan bisnis berdasarkan proses bisnis organisasi

KODE UNIT : **J.62KAM00.006.2**
JUDUL UNIT : **Mengimplementasikan Penyediaan Fasilitas Pemrosesan Informasi dengan Redundansi yang sesuai**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengimplementasikan penyediaan fasilitas pemrosesan informasi dengan redundansi yang sesuai melalui penentuan persyaratan redundansi untuk Ketersediaan layanan bisnis dan penerapan arsitektur sistem dengan redundansi yang sesuai.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menentukan persyaratan redundansi untuk Ketersediaan fasilitas pemrosesan informasi	1.1 **Persyaratan redundansi** diidentifikasi sesuai dengan **kebutuhan layanan bisnis**. 1.2 Persyaratan redundansi untuk **Ketersediaan fasilitas pemrosesan informasi** disusun sesuai dengan hasil identifikasi.
2. Menerapkan arsitektur sistem dengan redundansi yang sesuai	2.1 **Arsitektur sistem** dirancang sesuai dengan persyaratan redundansi. 2.2 Arsitektur sistem dengan redundansi dilaksanakan sesuai rancangan arsitektur sistem.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk menentukan persyaratan redundansi untuk Ketersediaan fasilitas pemrosesan informasi dan menerapkan arsitektur sistem dengan redundansi yang sesuai.
   1.2 Persyaratan redundansi merujuk pada persyaratan yang harus dipenuhi untuk memastikan bahwa sistem atau layanan TIK tersedia dengan tingkat yang memadai, sehingga operasional bisnis dapat berjalan secara efektif dan tidak terganggu.
   1.3 Kebutuhan layanan bisnis merujuk pada persyaratan yang harus dipenuhi oleh sistem atau layanan TIK untuk mendukung operasional bisnis dan memenuhi Kebutuhan Keamanan Informasi.
   1.4 Ketersediaan fasilitas pemrosesan informasi merujuk pada kemampuan fasilitas pemrosesan informasi untuk tetap tersedia dan dapat dimanfaatkan oleh pengguna yang berwenang sesuai dengan kebutuhan bisnis.
   1.5 Arsitektur sistem merujuk pada desain dan struktur sistem informasi yang mencakup infrastruktur teknologi, perangkat lunak, jaringan, komponen, dan/atau interaksi yang ada dalam lingkungan TIK suatu organisasi.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer atau perangkat pengolahan data
      2.1.2 Media penyimpanan data
      2.1.3 Internet

2.2 Perlengkapan
2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
(Tidak ada.)

4. Norma dan standar
4.1 Norma
(Tidak ada.)
4.2 Standar
4.2.1 SNI ISO/IEC 27001 Keamanan Informasi, keamanan siber, dan proteksi privasi – Sistem manajemen Keamanan Informasi – Persyaratan
4.2.2 SNI ISO/IEC 27002 Keamanan Informasi, keamanan siber, dan proteksi privasi – Kontrol Keamanan Informasi

PANDUAN PENILAIAN

1. Konteks penilaian
1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
3.1 Pengetahuan
3.1.1 Desain arsitektur sistem
3.2 Keterampilan
3.2.1 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami dalam menjabarkan rencana kesiapan TIK dalam mendukung organisasi

4. Sikap kerja yang diperlukan
4.1 Cermat dalam mengidentifikasi persyaratan redundansi yang sesuai
4.2 Teliti dalam mengidentifikasi persyaratan redundansi yang sesuai
4.3 Berpikir sistematis dalam merancang arsitektur sistem yang sesuai

5. Aspek kritis
5.1 Ketepatan dalam mengidentifikasi persyaratan redundansi untuk Ketersediaan fasilitas pemrosesan informasi

KODE UNIT : **J.62KAM00.007.1**
JUDUL UNIT : **Menetapkan Metode Autentikasi**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengidentifikasi risiko dan menentukan metode Autentikasi yang akan digunakan untuk validasi transmisi, pesan atau sumber aslinya.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi risiko pada transmisi, pesan atau sumber aslinya	1.1 Informasi terkait **risiko** transmisi, pesan atau sumber aslinya diinventarisasi berdasarkan Kebutuhan Keamanan Informasi. 1.2 Hasil inventarisasi risiko transmisi, pesan atau sumber aslinya dipilih berdasarkan Kebutuhan Keamanan Informasi.
2. Menentukan metode Autentikasi yang akan digunakan untuk validasi transmisi, pesan atau sumber aslinya yang terpercaya	2.1 **Metode Autentikasi** diinventarisasi berdasarkan risiko. 2.2 Metode Autentikasi dipilih berdasarkan praktik terbaik Keamanan Informasi.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk mengidentifikasi risiko pada transmisi, pesan atau sumber aslinya dan mengidentifikasi metode Autentikasi yang akan digunakan untuk validasi transmisi, pesan atau sumber aslinya yang terpercaya.
   1.2 Risiko merupakan sesuatu kejadian yang mengacu pada potensi terjadinya kerugian atau bahaya terkait dengan kebocoran, perusakan, atau akses yang tidak sah terhadap informasi yang penting dan bernilai serta melibatkan ancaman terhadap Kerahasiaan, Integritas, dan Ketersediaan data atau sistem informasi, seperti: kebocoran informasi, perusakan informasi, akses yang tidak sah, Kerahasiaan, Integritas, Ketersediaan, dan lain-lain.
   1.3 Metode Autentikasi meliputi:
      1.3.1 Metode Autentikasi identitas merupakan cara untuk memverifikasi dan memastikan identitas pengguna sebelum memberikan akses ke sistem atau layanan tertentu yang akan digunakan dalam proses identifikasi dan verifikasi pada transmisi, pesan atau sumber aslinya. Metode Autentikasi umum yang digunakan: Autentikasi dengan kata sandi (*password authentication*), Autentikasi dengan faktor ganda (*multi-factor authentication*), Autentikasi dengan kunci fisik (*physical key authentication*), Autentikasi dengan sertifikat digital (*digital certificate authentication*), dan Autentikasi dengan biometrik (*biometric authentication*).
      1.3.2 Metode Autentikasi informasi merupakan proses memverifikasi dan memastikan bahwa informasi atau data yang diberikan atau diterima benar, asli, dan berasal dari sumber yang sah. Tujuannya adalah untuk mengurangi risiko manipulasi, pemalsuan, atau penyebaran informasi palsu. Beberapa metode Autentikasi informasi yang umum digunakan meliputi: tanda

tangan digital, sertifikat digital, penggunaan sandi dan kata sandi, *Virtual Private Network* (VPN), biometrik, token *One-Time Password* (OTP), penandatanganan, dan cap waktu.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer atau perangkat pengolahan data
      2.1.2 Internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)
   4.2 Standar
      (Tidak ada.)

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Klasifikasi informasi
      3.1.2 Ruang lingkup metode Autentikasi
   3.2 Keterampilan
      3.2.1 Mengolah hasil inventarisasi risiko transmisi, pesan atau sumber aslinya

4. Sikap kerja yang diperlukan
   4.1 Berintegritas dalam menjaga informasi terkait risiko transmisi, pesan atau sumber aslinya
   4.2 Teliti dalam menginventarisasi risiko transmisi, pesan, atau sumber aslinya
   4.3 Objektif dalam menentukan metode Autentikasi yang akan digunakan

5. Aspek kritis
   5.1 Ketepatan dalam memilih metode Autentikasi berdasarkan praktik terbaik Keamanan Informasi

KODE UNIT : **J.62KAM00.008.1**
JUDUL UNIT : **Melaksanakan Autentikasi dalam Upaya Mencegah Peniruan Identitas**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melakukan verifikasi identitas dalam upaya mencegah peniruan identitas dan mendokumentasikan hasil Autentikasi untuk verifikasi transmisi, pesan, atau sumber aslinya yang terpercaya.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Melakukan verifikasi identitas dalam upaya mencegah peniruan identitas	1.1 Setiap **identitas** diverifikasi sesuai dengan **kriteria Autentikasi**. 1.2 Informasi terkait peniruan identitas divalidasi berdasarkan kriteria Autentikasi.
2. Mendokumentasikan hasil Autentikasi untuk verifikasi identitas	2.1 Identitas diverifikasi berdasarkan **metode Autentikasi identitas**. 2.2 Hasil verifikasi dicatat berdasarkan Kebutuhan Keamanan Informasi.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk melakukan verifikasi identitas dalam upaya mencegah peniruan identitas dan mendokumentasikan hasil Autentikasi untuk verifikasi transmisi, pesan atau sumber aslinya yang terpercaya.
   1.2 Identitas merupakan kunci untuk memastikan bahwa hanya entitas yang berwenang yang dapat mengakses sumber daya atau melakukan tindakan tertentu dalam lingkungan yang aman. Identitas mengacu pada cara untuk memverifikasi dan mengenali entitas (seseorang atau perangkat) yang terlibat dalam akses atau interaksi dengan sistem atau data. Definisi identitas dalam Keamanan Informasi meliputi atribut-atribut berikut:
      1.2.1 Nama pengguna (*username*).
      1.2.2 Kredensial pengguna (*credentials*).
      1.2.3 Profil pengguna (*user profile*).
      1.2.4 Identitas digital (*digital identity*).
      1.2.5 Metode Autentikasi (*authentication method*).
      1.2.6 Audit identitas (*identity audit*).
   1.3 Kriteria Autentikasi merupakan ukuran yang menjadi dasar penilaian atau penetapan dari metode Autentikasi yang digunakan dan mengacu pada persyaratan yang harus dipenuhi oleh metode Autentikasi untuk dianggap efektif dan aman. Beberapa kriteria umum untuk Autentikasi meliputi:
      1.3.1 Tingkat keamanan yang memadai untuk melindungi sistem atau layanan dari akses yang tidak sah.
      1.3.2 Keunikan identitas pengguna.
      1.3.3 Mudah digunakan.
      1.3.4 Skalabilitas.
      1.3.5 Kecepatan dan kinerja.
      1.3.6 Kehandalan.
      1.3.7 Privasi dan kerahasian.
      1.3.8 Faktor biaya.

1.4 Metode Autentikasi identitas merupakan cara untuk memverifikasi dan memastikan identitas pengguna sebelum memberikan akses ke sistem atau layanan tertentu yang akan digunakan dalam proses identifikasi dan verifikasi pada transmisi, pesan atau sumber aslinya. Metode Autentikasi umum yang digunakan meliputi:
   1.4.1 Autentikasi dengan kata sandi (*password authentication*).
   1.4.2 Autentikasi dengan faktor ganda (*multi-factor authentication*).
   1.4.3 Autentikasi dengan kunci fisik (*physical key authentication*).
   1.4.4 Autentikasi dengan sertifikat digital (*digital certificate authentication*).
   1.4.5 Autentikasi dengan biometrik (*biometric authentication*).

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer atau perangkat pengolahan data
      2.1.2 Aplikasi Autentikasi
      2.1.3 Jaringan komputer
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)
   4.2 Standar
      (Tidak ada.)

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Klasifikasi informasi
      3.1.2 Ruang lingkup metode Autentikasi
   3.2 Keterampilan
      3.2.1 Melakukan verifikasi identitas berdasarkan kriteria Autentikasi

4. Sikap kerja yang diperlukan
   4.1 Berintegritas dalam menjaga informasi terkait identitas yang diverifikasi
   4.2 Teliti dalam melakukan verifikasi identitas
   4.3 Objektif dalam melakukan verifikasi identitas

5. Aspek kritis
   5.1 Ketepatan dalam memverifikasi identitas berdasarkan metode Autentikasi identitas

KODE UNIT : **J.62KAM00.009.1**
JUDUL UNIT : **Melaksanakan Autentikasi dalam Upaya Mencegah Pemalsuan Informasi**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melaksanakan Autentikasi dalam upaya mencegah pemalsuan informasi melalui validasi dan dokumentasi hasil Autentikasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Melakukan validasi dalam upaya mencegah pemalsuan informasi	1.1 **Kriteria Autentikasi** ditentukan berdasarkan **kategori klasifikasi informasi**. 1.2 Setiap pemalsuan informasi divalidasi sesuai dengan kriteria Autentikasi.
2. Mendokumentasikan hasil Autentikasi untuk validasi informasi	2.1 Informasi divalidasi berdasarkan **metode Autentikasi informasi.** 2.2 Hasil validasi dicatat berdasarkan Kebutuhan Keamanan Informasi.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk melakukan validasi dalam upaya mencegah pemalsuan informasi dan mendokumentasikan hasil Autentikasi untuk validasi informasi.
   1.2 Kriteria Autentikasi merupakan ukuran yang menjadi dasar penilaian atau penetapan dari metode Autentikasi yang digunakan dan mengacu pada persyaratan yang harus dipenuhi oleh metode Autentikasi untuk dianggap efektif dan aman. Beberapa kriteria umum untuk Autentikasi meliputi tingkat keamanan yang memadai untuk melindungi sistem atau layanan dari akses yang tidak sah, keunikan identitas pengguna, mudah digunakan, skalabilitas, kecepatan dan kinerja, kehandalan, privasi dan kerahasian, serta faktor biaya.
   1.3 Kategori klasifikasi informasi merupakan pengkategorian/penggolongan informasi berdasarkan pada tingkat keseriusan dampak yang ditimbulkan terhadap kepentingan dan keamanan negara, publik dan perorangan. Kategori klasifikasi dapat merujuk standar antara lain:
      a. SNI ISO/IEC 27001 Keamanan Informasi, keamanan siber, dan proteksi privasi – Sistem manajemen Keamanan Informasi – Persyaratan.
      b. SNI ISO/IEC 27002 Keamanan Informasi, keamanan siber, dan proteksi privasi – Kontrol Keamanan Informasi, NIST SP 800-53 *Security and Privacy Controls for Information Systems and Organizations*, *Center for Internet Security – Critical Security Controls* (CIS – CSC).
      c. Standar yang berlaku lainnya.
   1.4 Metode Autentikasi informasi merupakan proses memverifikasi dan memastikan bahwa informasi atau data yang diberikan atau diterima benar, asli, dan berasal dari sumber yang sah. Tujuannya adalah untuk mengurangi risiko manipulasi, pemalsuan, atau penyebaran informasi palsu. Beberapa metode Autentikasi informasi yang umum digunakan meliputi tanda tangan digital, sertifikat digital, penggunaan

sandi dan kata sandi, *Virtual Private Network* (VPN), penandatanganan dan cap waktu, biometrik, dan token *One-Time Password* (OTP).

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer atau perangkat pengolahan data
      2.1.2 Aplikasi Autentikasi
      2.1.3 Jaringan Komputer
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)
   4.2 Standar
      4.2.1 SNI ISO/IEC 27001 Keamanan Informasi, keamanan siber, dan proteksi privasi – Sistem manajemen Keamanan Informasi – Persyaratan.
      4.2.2 SNI ISO/IEC 27002 Keamanan Informasi, keamanan siber, dan proteksi privasi – Kontrol Keamanan Informasi, NIST SP 800-53 *Security and Privacy Controls for Information Systems and Organizations*, *Center for Internet Security – Critical Security Controls* (CIS – CSC).

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Klasifikasi informasi
      3.1.2 Ruang lingkup metode Autentikasi
   3.2 Keterampilan
      3.2.1 Melakukan validasi informasi berdasarkan kriteria Autentikasi

4. Sikap kerja yang diperlukan
   4.1 Berintegritas dalam menjaga informasi yang divalidasi

4.2 Teliti dalam melakukan validasi informasi
4.3 Objektif dalam melakukan validasi informasi

5. Aspek kritis
5.1 Ketepatan dalam memvalidasi informasi berdasarkan metode Autentikasi informasi

KODE UNIT : **J.62KAM00.010.1**
JUDUL UNIT : **Menentukan Aset Teknologi Informasi yang Dikontrol**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menentukan Aset Teknologi Informasi yang dikontrol melalui pencatatan Aset Teknologi Informasi dan penerapan kategori di setiap aset penting.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Melakukan pencatatan Aset Teknologi Informasi	1.1 Aset Teknologi Informasi diinventarisasi berdasarkan **proses bisnis organisasi.** 1.2 Daftar inventarisasi aset didokumentasikan sesuai **kategori** yang digunakan pada organisasi.
2. Menerapkan kategori di setiap aset penting	2.1 **Klasifikasi** Aset Teknologi Informasi ditentukan sesuai kategori yang digunakan pada organisasi. 2.2 Dokumentasi Aset Teknologi Informasi direkam berdasarkan klasifikasi aset.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk melakukan pencatatan Aset Teknologi Informasi dan menerapkan kategori di setiap aset penting.
   1.2 Proses bisnis organisasi merujuk pada serangkaian langkah atau aktivitas yang dilakukan untuk mencapai tujuan organisasi terkait Keamanan Informasi.
   1.3 Klasifikasi didasarkan pada tingkatan strategis atau kepentingan penggunaan Keamanan Informasi.
   1.4 Kategori meliputi organisasi, sumber daya manusia, fisik, dan teknologi.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer atau perangkat pengolahan data
      2.1.2 Internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Infomasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)

4.2 Standar
4.2.1 SNI ISO/IEC 27001 Keamanan Informasi, keamanan siber, dan proteksi privasi – Sistem manajemen Keamanan Informasi – Persyaratan
4.2.2 SNI ISO/IEC 27002 Keamanan Informasi, keamanan siber, dan proteksi privasi – Kontrol Keamanan Informasi

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Tata kelola Keamanan Informasi
      3.1.2 Manajemen Keamanan Informasi
   3.2 Keterampilan
      3.2.1 Melakukan pencatatan dan menerapkan kategorisasi

4. Sikap kerja yang diperlukan
   4.1 Teliti dalam melakukan pencatatan Aset Teknologi Informasi dan menerapkan kategori di setiap aset penting

5. Aspek kritis
   5.1 Ketepatan dalam menentukan klasifikasi dari Aset Teknologi Informasi sesuai kategori yang digunakan pada organisasi

KODE UNIT : **J.62KAM00.011.2**
JUDUL UNIT : **Melaksanakan Pengontrolan Akses Pengguna yang Berwenang**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melaksanakan pengontrolan akses pengguna yang berwenang melalui pemeriksaan ketentuan hak akses pengguna dan pemantauan terhadap aktivitas pelanggaran.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Memeriksa ketentuan hak akses pengguna	1.1 Jenis **kontrol akses** dipilih sesuai Kebutuhan Keamanan Informasi. 1.2 **Basis data pengguna** dibuat sesuai dengan kontrol akses.
2. Melakukan pemantauan terhadap aktivitas pelanggaran	2.1 Jenis aktivitas pengguna diidentifikasi sesuai dengan kewenangan. 2.2 **Pelanggaran kewenangan** direkam sesuai dengan Kebutuhan Keamanan Informasi.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk memeriksa ketentuan hak akses pengguna dan melakukan pemantauan terhadap aktivitas pelanggaran.
   1.2 Kontrol akses meliputi *Role-Based Access Control* (RBAC), *Attribute-Based Access Control* (ABAC), *Policy Based Access Control* (PBAC), *Access Control List* (ACL), *Mandatory Access Control* (MAC), *Discretionary Access Control* (DAC), *Time Based Access Control* (TBAC), dan lain-lain.
   1.3 Basis data pengguna (*user database*) merupakan sekumpulan informasi atau data yang berkaitan dengan pengguna dari suatu sistem atau layanan. Basis data ini menyimpan berbagai informasi yang berkaitan dengan pengguna, seperti nama, alamat, nomor telepon, alamat email, *username*, *password*, preferensi, riwayat transaksi, dan lain sebagainya.
   1.4 Pelanggaran kewenangan meliputi serangan *brute-force attack*, pencurian kredensial, penyalahgunaan hak akses, *man-in-the-middle attack*, *social engineering* dan penyebaran *malware*.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer atau perangkat pengolah data
      2.1.2 Jaringan komputer
      2.1.3 Aplikasi kontrol akses
      2.1.4 Aplikasi penyimpanan *log*
   2.2 Perlengkapan
      2.2.1 Media penyimpanan

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Infomasi dan Transaksi Elektronik

3.2 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
      4.2.1 SNI ISO/IEC 27001 Keamanan Informasi, keamanan siber, dan proteksi privasi – Sistem manajemen Keamanan Informasi – Persyaratan
      4.2.2 SNI ISO/IEC 27002 Keamanan Informasi, keamanan siber, dan proteksi privasi – Kontrol Keamanan Informasi

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Hak akses
   3.2 Keterampilan
      3.2.1 Melakukan pemantauan aktivitas akses pengguna

4. Sikap kerja yang diperlukan
   4.1 Teliti dalam memeriksa ketentuan hak akses pengguna
   4.2 Objektif dalam melakukan pemantauan terhadap aktivitas pelanggaran.

5. Aspek kritis
   5.1 Ketepatan dalam mengidentifikasi jenis aktivitas pengguna sesuai dengan kewenangan

KODE UNIT : **J.62KAM00.012.2**
JUDUL UNIT : **Memilih Metode Pelindungan Fisik Keamanan Informasi**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menentukan metode pelindungan fisik Keamanan Informasi melalui identifikasi ancaman fisik dan metode pelindungan fisik.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi ancaman fisik Keamanan Informasi	1.1 **Topologi lingkungan organisasi** diinventarisasi sesuai Kebutuhan Keamanan Informasi. 1.2 **Daftar ancaman fisik Keamanan Informasi** disusun berdasarkan topologi lingkungan organisasi.
2. Mengidentifikasi metode pelindungan fisik Keamanan Informasi	2.1 **Tingkat pelindungan fisik** diinventarisasi berdasarkan daftar ancaman fisik Keamanan Informasi. 2.2 **Metode pengamanan fisik** dipilih sesuai tingkat pelindungan fisik. 2.3 Daftar pengamanan fisik didokumentasikan sesuai dengan **format yang berlaku.**

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk melaksanakan langkah-langkah pelindungan terhadap lingkungan fisik organisasi dalam melindungi aset informasi dari ancaman fisik.
   1.2 Topologi lingkungan organisasi merupakan struktur atau konfigurasi fisik dari komponen-komponen teknologi informasi dalam lingkungan organisasi seperti lokasi dan penempatan perangkat.
   1.3 Daftar ancaman fisik Keamanan Informasi merupakan segala sesuatu yang berpotensi menyebabkan gangguan terhadap lingkungan fisik organisasi sehingga mengalami kerusakan dan kerugian organisasi.
   1.4 Tingkat pelindungan fisik merupakan suatu ukuran yang merujuk pada sejauh mana suatu sistem, perangkat, atau area dapat dilindungi dari ancaman atau gangguan fisik dari pihak luar.
   1.5 Metode pengamanan fisik merupakan serangkaian tindakan, strategi, atau langkah-langkah yang diambil untuk melindungi lingkungan fisik suatu organisasi dari ancaman dan risiko keamanan fisik sesuai standar.
   1.6 Format yang berlaku yaitu standar atau aturan dalam hal tata letak, struktur, dan penulisan dokumen yang konsisten dan sesuai dengan kebijakan dan pedoman yang ditetapkan oleh organisasi.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer atau perangkat pengolahan data
      2.1.2 Tata ruang bangunan fisik
      2.1.3 Jaringan komputer
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
       (Tidak ada.)
   4.2 Standar
       4.2.1 SNI ISO/IEC 27001 Keamanan Informasi, keamanan siber, dan proteksi privasi – Sistem manajemen Keamanan Informasi – Persyaratan
       4.2.2 SNI ISO/IEC 27005 - *Information security, cybersecurity and privacy protection - Guidance on managing information security risks* dan NIST SP 800-53 - *Security and Privacy Controls for Information Systems and Organizations*.

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
       3.1.1 Persyaratan keamanan fisik
       3.1.2 Metode pengamanan fisik
   3.2 Keterampilan
       3.2.1 Mengidentifikasi risiko
       3.2.2 Menggunakan aplikasi pengolah data

4. Sikap kerja yang diperlukan
   4.1 Berintegritas dalam menjaga informasi terkait dengan topologi lingkungan organisasi yang diamankan
   4.2 Teliti dalam mengidentifikasi risiko fisik pada topologi lingkungan organisasi
   4.3 Objektif dalam menentukan metode pengamanan fisik yang dibutuhkan sesuai risiko yang diidentifikasi

5. Aspek kritis
   5.1 Ketepatan dalam memilih metode pelindungan fisik berdasarkan tingkat pelindungan fisik

KODE UNIT : **J.62KAM00.013.2**
JUDUL UNIT : **Menyusun Rencana Pelaksanaan Pelindungan Fisik Keamanan Informasi**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menyusun rencana pelaksanaan pelindungan fisik Keamanan Informasi melalui identifikasi keberadaan entitas pada area pengamanan fisik dan penentuan rencana pelaksanaan pelindungan fisik Keamanan Informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi keberadaan entitas pada area pengamanan fisik	1.1 Daftar aktivitas **entitas** pada **lingkungan organisasi** diinventarisasi berdasarkan **daftar ancaman fisik.** 1.2 Daftar aktivitas entitas dianalisis sesuai **kebutuhan keamanan fisik.** 1.3 Daftar aktivitas entitas dibuat berdasarkan format yang berlaku.
2. Menentukan rencana pelaksanaan pelindungan fisik Keamanan Informasi	2.1 Rencana pelaksanaan pelindungan fisik disusun berdasarkan kebutuhan keamanan fisik. 2.2 Rencana pelaksanaan pelindungan fisik Keamanan Informasi didokumentasikan sesuai **format yang berlaku.**

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk melaksanakan langkah-langkah identifikasi keberadaan entitas pada area pengamanan fisik dalam melakukan pelindungan fisik.
   1.2 Entitas merupakan suatu objek yang berada di dalam lingkungan fisik dan memiliki nilai atau kepentingan yang perlu dilindungi. Entitas dapat berupa makhluk hidup dan perangkat keras.
   1.3 Lingkungan organisasi merupakan seluruh area fisik atau tempat organisasi beroperasi yang mencakup semua bangunan, fasilitas, ruangan, atau tempat lain yang digunakan oleh organisasi untuk melakukan kegiatannya dan membutuhkan pelindungan fisik.
   1.4 Daftar ancaman fisik merupakan segala sesuatu yang berpotensi menyebabkan gangguan terhadap lingkungan fisik organisasi sehingga mengalami kerusakan dan kerugian organisasi.
   1.5 Kebutuhan keamanan fisik merupakan persyaratan atau aspek yang harus dipenuhi dalam melindungi lingkungan fisik organisasi untuk mencegah, mengurangi, atau mengatasi ancaman dan risiko keamanan fisik yang mungkin terjadi sesuai dengan standar.
   1.6 Format yang berlaku merupakan standar atau aturan dalam hal tata letak, struktur, dan penulisan dokumen yang konsisten dan sesuai dengan kebijakan dan pedoman yang ditetapkan oleh organisasi.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer atau perangkat pengolahan data

2.2 Perlengkapan
2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
(Tidak ada.)

4. Norma dan standar
4.1 Norma
(Tidak ada.)
4.2 Standar
4.2.1 SNI ISO/IEC 27001 Keamanan Informasi, keamanan siber, dan proteksi privasi – Sistem manajemen Keamanan Informasi – Persyaratan
4.2.2 SNI ISO/IEC 27005 - *Information security, cybersecurity and privacy protection - Guidance on managing information security risks* dan NIST SP 800-53 - *Security and Privacy Controls for Information Systems and Organizations*

PANDUAN PENILAIAN

1. Konteks penilaian
1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
3.1 Pengetahuan
3.1.1 Persyaratan keamanan fisik
3.1.2 Metode pengamanan fisik
3.2 Keterampilan
3.2.1 Menggunakan aplikasi pengolah data

4. Sikap kerja yang diperlukan
4.1 Berintegritas dalam menjaga informasi terkait dengan daftar aktivitas entitas pada lingkungan organisasi yang diamankan
4.2 Teliti dalam mendata seluruh aktivitas entitas sesuai kebutuhan keamanan fisik organisasi
4.3 Objektif dalam merencanakan pelaksanaan pelindungan fisik organisasi

5. Aspek kritis
5.1 Ketepatan dalam membuat rencana pelaksanaan pelindungan fisik berdasarkan kebutuhan keamanan fisik

KODE UNIT : **J.62KAM00.014.2**
JUDUL UNIT : **Memetakan Profil Sumber Daya Manusia Keamanan Informasi**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam memetakan profil Sumber Daya Manusia (SDM) Keamanan Informasi sesuai dengan profil risiko Keamanan Informasi organisasi dan pembagian peran dalam mitigasi risiko organisasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menentukan profil SDM sesuai dengan profil risiko Keamanan Informasi organisasi	1.1 **Profil SDM** diobservasi berdasarkan **profil risiko organisasi.** 1.2 Profil SDM dipetakan dengan profil risiko organisasi. 1.3 Pemetaan profil SDM didokumentasikan berdasarkan Kebutuhan Keamanan Informasi.
2. Menyusun pembagian peran sesuai profil SDM	2.1 Peran jabatan Keamanan Informasi organisasi diidentifikasi sesuai pemetaan profil SDM. 2.2 **Dokumen peran jabatan** Keamanan Informasi organisasi dibuat berdasarkan pemetaan profil SDM.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk menentukan profil SDM sesuai dengan profil risiko Keamanan Informasi organisasi dan menyusun pembagian peran sesuai profil SDM.
   1.2 Profil SDM meliputi informasi mengenai karyawan atau anggota tim yang bekerja di organisasi tersebut. Profil SDM mencakup berbagai data dan informasi yang membantu organisasi dalam mengelola dan mengoptimalkan potensi dan kinerja karyawan. Beberapa komponen dalam profil sumber daya manusia organisasi meliputi informasi pribadi, kualifikasi dan pendidikan, pengalaman kerja, kompetensi dan keterampilan, daftar keterampilan, evaluasi kinerja, penghargaan dan pengakuan, pengembangan karir, catatan pelatihan, data kepegawaian, riwayat kesehatan, serta keikutsertaan dan partisipasi.
   1.3 Profil risiko organisasi merupakan gambaran menyeluruh atas besarnya potensi risiko yang melekat pada seluruh portofolio atau eksposur organisasi yang mencakup domain fisik, logika, dan organisasional.
   1.4 Dokumen peran jabatan yang dimaksud berupa dokumen yang menjelaskan tentang penentuan tugas, tanggung jawab, dan ekspektasi untuk setiap posisi dalam suatu organisasi, menguraikan bidang-bidang utama fokus dan memberikan kejelasan bagi karyawan.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer atau perangkat pengolahan data
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
       (Tidak ada.)
   4.2 Standar
       4.2.1 SNI SNI ISO/IEC 27001 Teknologi informasi – Teknik keamanan – Sistem manajemen Keamanan Informasi – Persyaratan
       4.2.2 SNI ISO/IEC 27002 Keamanan Informasi, keamanan siber, dan proteksi privasi – Kontrol Keamanan Informasi

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
       3.1.1 Manajemen risiko organisasi
       3.1.2 Kode etik dan keprofesian
   3.2 Keterampilan
       3.2.1 Mengolah kata–kata untuk dapat membuat penjelasan yang mudah dipahami dalam menjabarkan profil SDM dan peran jabatan Keamanan Informasi organisasi

4. Sikap kerja yang diperlukan
   4.1 Objektif dalam menentukan profil SDM Keamanan Informasi organisasi dan pembagian peran jabatan
   4.2 Teliti dalam menentukan profil SDM Keamanan Informasi organisasi dan pembagian peran jabatan
   4.3 Berpikir sistematis dalam menentukan profil SDM Keamanan Informasi organisasi dan pembagian peran jabatan

5. Aspek kritis
   5.1 Ketepatan dalam mengidentifikasi peran jabatan Keamanan Informasi organisasi sesuai pemetaan profil SDM

KODE UNIT : **J.62KAM00.015.1**
JUDUL UNIT : **Menyusun Dokumen Skrining Personel Keamanan Informasi**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menyusun dokumen skrining personel Keamanan Informasi melalui penentuan kriteria skrining personel Keamanan Informasi dan perancangan instrumen skrining personel Keamanan Informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menentukan kriteria skrining personel Keamanan Informasi	1.1 **Kriteria skrining personel Keamanan Informasi** diidentifikasi sesuai dengan **dokumen peran jabatan**. 1.2 Kriteria skrining personel Keamanan Informasi dipilih sesuai Kebutuhan Keamanan Informasi.
2. Merancang instrumen skrining personel Keamanan Informasi	2.1 Daftar pertanyaan instrumen skrining dibuat sesuai parameter kriteria skrining personel Keamanan Informasi. 2.2 **Mekanisme pengukuran instrumen skrining** dibuat sesuai dengan daftar pertanyaan instrumen skrining. 2.3 Instrumen skrining personel Keamanan Informasi didokumentasikan sesuai dengan **format yang berlaku.**

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk menentukan kriteria skrining personel Keamanan Informasi dan merancang instrumen skrining personel Keamanan Informasi.
   1.2 Kriteria skrining personel Keamanan Informasi merupakan evaluasi yang dilakukan sebagai bagian dari survei atau tes untuk melihat kesesuaian seseorang pada pekerjaan tertentu meliputi kompetensi, daftar riwayat hidup, kualifikasi, identitas yang dikeluarkan oleh otoritas yang berwenang, latar belakang sosial, riwayat hukum.
   1.3 Dokumen peran jabatan yang dimaksud berupa dokumen yang menjelaskan tentang penentuan tugas, tanggung jawab, dan ekspektasi untuk setiap posisi dalam suatu organisasi, menguraikan bidang-bidang utama fokus dan memberikan kejelasan bagi karyawan.
   1.4 Mekanisme pengukuran instrumen skrining merujuk pada cara atau prosedur yang digunakan untuk mengukur atau menilai suatu variabel atau karakteristik dalam rangka melakukan skrining atau penyaringan terhadap individu atau objek tertentu.
   1.5 Format yang berlaku yaitu standar atau aturan dalam hal terminologi tata letak, struktur, dan penulisan dokumen yang konsisten dan sesuai dengan kebijakan dan pedoman yang ditetapkan oleh organisasi.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer atau perangkat pengolah data
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)
   4.2 Standar
      4.2.1 SNI ISO/IEC 27001 Keamanan Informasi, keamanan siber, dan proteksi privasi – Sistem manajemen Keamanan Informasi – Persyaratan
      4.2.2 SNI ISO/IEC 27002 Keamanan Informasi, keamanan siber, dan proteksi privasi – Kontrol Keamanan Informasi

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 *Security clearance*
      3.1.2 Kompetensi personil Keamanan Informasi
   3.2 Keterampilan
      3.2.1 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami dalam menyusun instrumen skrining personel Keamanan Informasi

4. Sikap kerja yang diperlukan
   4.1 Objektif dalam menentukan kriteria skrining personel dan merancang instrumen skrining personel Keamanan Informasi
   4.2 Cermat dalam menentukan kriteria skrining personel dan merancang instrumen skrining personel Keamanan Informasi

5. Aspek kritis
   5.1 Ketepatan dalam mengidentifikasi kriteria skrining personel Keamanan Informasi sesuai dengan dokumen peran jabatan

KODE UNIT : **J.62KAM00.016.1**
JUDUL UNIT : **Menerapkan Teknologi Keamanan Informasi sesuai dengan Ketentuan yang Berlaku**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menerapkan teknologi Keamanan Informasi sesuai dengan ketentuan yang berlaku melalui penentuan teknologi Keamanan Informasi yang dibutuhkan dan penyusunan prosedur penggunaan teknologi Keamanan Informasi berdasarkan kebijakan yang ditentukan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menentukan teknologi Keamanan Informasi	1.1 Teknologi Keamanan Informasi diidentifikasi berdasarkan Kebutuhan Keamanan Informasi. 1.2 Teknologi Keamanan Informasi dipilih berdasarkan prioritas Kebutuhan Keamanan Informasi.
2. Menyusun prosedur penggunaan teknologi Keamanan Informasi	2.1 Prosedur penggunaan teknologi Keamanan Informasi dibuat berdasarkan **kebijakan Keamanan Informasi** organisasi. 2.2 Prosedur penggunaan teknologi Keamanan Informasi direviu berdasarkan periode tertentu.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk menentukan teknologi Keamanan Informasi yang dibutuhkan dan menyusun prosedur penggunaan teknologi Keamanan Informasi berdasarkan kebijakan yang sudah ditentukan.
   1.2 Kebijakan Keamanan Informasi merupakan kebijakan di bidang Keamanan Informasi yang ditetapkan oleh pimpinan guna mendukung tercapainya tujuan organisasi yang mencakup tujuan Keamanan Informasi beserta kerangka kerja penerapannya serta komitmen pemenuhan persyaratan teknologi Keamanan Informasi dan pengembangannya.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer atau perangkat pengolahan data
      2.1.2 Jaringan komputer
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)

4.2 Standar
4.2.1 SNI ISO/IEC 27001 Keamanan Informasi, keamanan siber, dan proteksi privasi – Sistem manajemen Keamanan Informasi – Persyaratan
4.2.2 SNI ISO/IEC 27002 Keamanan Informasi, keamanan siber, dan proteksi privasi - Kontrol Keamanan Informasi

PANDUAN PENILAIAN

1. Konteks penilaian
1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
3.1 Pengetahuan
3.1.1 Pengamanan informasi mencakup Kerahasiaan, Integritas, dan Autentikasi
3.1.2 Risiko dan manajemen risiko
3.1.3 Manajemen aset
3.1.4 Kendali akses
3.1.5 Taksonomi teknologi Keamanan Informasi
3.1.6 Perangkat teknologi Keamanan Informasi
3.2 Keterampilan
3.2.1 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami dalam menyusun prosedur penggunaan teknologi Keamanan Informasi

4. Sikap kerja yang diperlukan
4.1 Teliti dalam mengidentifikasi teknologi Keamanan Informasi
4.2 Berhati-hati dalam memilih teknologi Keamanan Informasi yang tepat guna
4.3 Sistematis dalam membuat prosedur penggunaan teknologi Keamanan Informasi
4.4 Konsisten dalam melakukan uji coba perangkat teknologi Keamanan Informasi
4.5 Adaptif dengan perkembangan teknologi Keamanan Informasi

5. Aspek kritis
5.1 Ketepatan dalam memilih teknologi Keamanan Informasi berdasarkan prioritas Kebutuhan Keamanan Informasi

KODE UNIT : **J.62KAM00.017.2**
JUDUL UNIT : **Menyusun Rencana Penerapan Aspek Keamanan Informasi pada Pemutakhiran Teknologi Informasi**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menyusun rencana penerapan aspek Keamanan Informasi pada pemutakhiran teknologi informasi melalui penentuan teknologi informasi dan identifikasi persyaratan keamanan yang relevan terhadap karakteristik teknologi informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menentukan pemutakhiran teknologi informasi	1.1 Teknologi informasi diinventarisasi berdasarkan Kebutuhan Keamanan Informasi. 1.2 **Daftar teknologi informasi** dibuat berdasarkan hasil analisis **implikasi teknologi informasi**.
2. Menentukan persyaratan keamanan yang relevan terhadap pemutakhiran teknologi informasi	2.1 **Persyaratan keamanan** dianalisis sesuai **karakteristik teknologi informasi**. 2.2 Dokumen persyaratan keamanan dibuat sesuai hasil analisis. 2.3 Dokumen rencana penerapan aspek Keamanan Informasi dibuat berdasarkan dokumen persyaratan keamanan.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk menentukan pemutakhiran teknologi informasi terhadap program keamanan teknologi informasi dan mengidentifikasi persyaratan keamanan yang relevan terhadap kemampuan teknologi informasi.
   1.2 Daftar teknologi informasi meliputi teknologi yang baru dan/atau yang diremajakan.
   1.3 Implikasi teknologi informasi melingkupi dampak yang ditimbulkan terhadap sistem informasi yang ada meliputi kecepatan proses, perubahan Standar Operasional Prosedur (SOP), penambahan pengetahuan, biaya, penambahan sumber daya seperti *storage*.
   1.4 Persyaratan keamanan meliputi Kerahasiaan, Integritas, dan Ketersediaan.
   1.5 Karakteristik teknologi informasi mengacu pada atribut atau sifat-sifat tertentu yang dimiliki oleh teknologi informasi (TI) antara lain automasi, kemampuan pengolahan, konektivitas, keamanan, skalabilitas, integrasi, mudah digunakan, fleksibilitas, keterandalan, efisiensi energi, dan kemampuan analitik.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer atau perangkat pengolahan data
      2.1.2 Internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
       (Tidak ada.)
   4.2 Standar
       4.2.1 SNI ISO/IEC 27001 Keamanan Informasi, keamanan siber, dan proteksi privasi – Sistem manajemen Keamanan Informasi – Persyaratan

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
       3.1.1 Tata kelola Keamanan Informasi
   3.2 Keterampilan
       3.2.1 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami dalam menyusun kategorisasi teknologi informasi

4. Sikap kerja yang diperlukan
   4.1 Komprehensif dalam melakukan analisis implikasi teknologi informasi yang baru dan/atau yang diremajakan sesuai Kebutuhan Keamanan Informasi
   4.2 Cermat dalam menyusun daftar persyaratan keamanan yang relevan terhadap karakteristik teknologi informasi yang baru dan/atau teknologi yang diremajakan

5. Aspek kritis
   5.1 Ketepatan dalam menganalisis persyaratan keamanan sesuai karakteristik teknologi informasi

KODE UNIT : **J.62KAM00.018.2**
JUDUL UNIT : **Menyusun Rencana Penerapan Kebijakan Keamanan Informasi**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menyusun rencana penerapan kebijakan Keamanan Informasi melalui identifikasi persyaratan kebijakan Keamanan Informasi dan penentuan kebijakan Keamanan Informasi sesuai dengan kebutuhan organisasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi persyaratan kebijakan Keamanan Informasi	1.1 **Persyaratan regulasi** diinventarisasi berdasarkan **konsiderasi kebijakan Keamanan Informasi**. 1.2 **Persyaratan bisnis** diinventarisasi berdasarkan konsiderasi kebijakan Keamanan Informasi.
2. Menentukan kebijakan Keamanan Informasi	2.1 **Kebijakan Keamanan Informasi** dipilih sesuai dengan dokumen persyaratan Keamanan Informasi. 2.2 Pihak-pihak yang terkait kebijakan Keamanan Informasi ditentukan berdasarkan Kebutuhan Keamanan Informasi. 2.3 Dokumen rencana penerapan kebijakan Keamanan Informasi dibuat berdasarkan kebijakan Keamanan Informasi.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk menerapkan persyaratan kebijakan Keamanan Informasi, dan mengidentifikasi kebijakan Keamanan Informasi.
   1.2 Persyaratan regulasi merupakan ketentuan dalam regulasi/peraturan perundang-undangan yang harus dipenuhi dalam penyusunan kebijakan Keamanan Informasi.
   1.3 Konsiderasi kebijakan Keamanan Informasi merupakan faktor yang perlu dipertimbangkan dalam mengembangkan dan mengimplementasikan kebijakan Keamanan Informasi dalam suatu organisasi.
   1.4 Persyaratan bisnis merupakan ketentuan dalam bisnis organisasi yang harus dipenuhi dalam penyusunan kebijakan Keamanan Informasi.
   1.5 Kebijakan Keamanan Informasi mencakup definisi, sasaran Keamanan Informasi atau kerangka kerja untuk untuk menetapkan sasaran Keamanan Informasi, prinsip untuk memandu semua aktivitas yang berkaitan dengan Keamanan Informasi, komitmen untuk memenuhi persyaratan yang berlaku terkait Keamanan Informasi, komitmen peningkatan berkelanjutan atas sistem manajemen Keamanan Informasi, penugasan tanggung jawab manajemen Keamanan Informasi untuk berbagai peran yang didefinisikan, dan prosedur Keamanan Informasi untuk menangani pembebasan dan eksepsi.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer dan perangkat pengolahan data
      2.1.2 Internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)
   4.2 Standar
      4.2.1 SNI ISO/IEC 27001 Keamanan Informasi, keamanan siber, dan proteksi privasi – Sistem manajemen Keamanan Informasi – Persyaratan
      4.2.2 SNI ISO/IEC 27002 Keamanan Informasi, keamanan siber, dan proteksi privasi – Kontrol Keamanan Informasi

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Kebijakan Keamanan Informasi
   3.2 Keterampilan
      3.2.1 Menggunakan aplikasi pengolah kata
      3.2.2 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami dalam menyusun dokumen rencana penerapan kebijakan Keamanan Informasi

4. Sikap kerja yang diperlukan
   4.1 Cermat dalam mengidentifikasi persyaratan regulasi dan persyaratan bisnis
   4.2 Teliti dalam mengidentifikasi persyaratan regulasi dan persyaratan bisnis
   4.3 Berpikir sistematis dan terstruktur dalam merumuskan kebijakan Keamanan Informasi yang sesuai

5. Aspek kritis
   5.1 Ketepatan dalam memilih kebijakan Keamanan Informasi sesuai dengan dokumen persyaratan Keamanan Informasi

KODE UNIT : **J.62KAM00.019.2**
JUDUL UNIT : **Melaksanakan Pemantauan Penerapan Kebijakan Keamanan Informasi**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melaksanakan pemantauan penerapan kebijakan Keamanan Informasi melalui menentukan instrumen pemantauan dan melakukan pemantauan penerapan kebijakan Keamanan Informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menentukan instrumen pemantauan penerapan kebijakan Keamanan Informasi	1.1 **Instrumen pemantauan** diidentifikasi sesuai Kebutuhan Keamanan Informasi. 1.2 Instrumen pemantauan dipilih sesuai Kebutuhan Keamanan Informasi.
2. Melakukan pemantauan penerapan kebijakan Keamanan Informasi	2.1 Instrumen pemantauan diterapkan sesuai **kebijakan pemantauan**. 2.2 Hasil pemantauan penerapan kebijakan Keamanan Informasi didokumentasikan sesuai **format yang berlaku.**

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk menentukan instrumen pemantauan penerapan kebijakan Keamanan Informasi dan melaksanakan pemantauan penerapan kebijakan Keamanan Informasi.
   1.2 Instrumen pemantauan merujuk pada alat, sistem, atau teknologi yang digunakan untuk memantau dan mengawasi penerapan kebijakan Keamanan Informasi dalam suatu organisasi.
   1.3 Kebijakan pemantauan dapat berupa waktu dan ruang lingkup pelaksanaan pemantauan yang dilakukan di tingkat manajemen, secara rutin atau periodik dan pada sebagian atau keseluruhan organisasi.
   1.4 Format yang berlaku merujuk dari panduan/tata naskah dinas pada organisasi.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer atau perangkat pengolahan data
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)

4.2 Standar
4.2.1 SNI ISO/IEC 27001 Keamanan Informasi, keamanan siber, dan proteksi privasi - Sistem manajemen Keamanan Informasi - Persyaratan
4.2.2 SNI ISO/IEC 27002 Keamanan Informasi, keamanan siber, dan proteksi privasi - Kontrol Keamanan Informasi

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Kebijakan Keamanan Informasi
   3.2 Keterampilan
      3.2.1 Meneliti secara cermat dengan kebijakan-kebijakan yang sudah ditetapkan dengan pelaksanaan dari kebijakan-kebijakan tersebut

4. Sikap kerja yang diperlukan
   4.1 Cermat dalam mengidentifikasi instrumen pemantauan yang sesuai
   4.2 Berpikir sistematis dalam merancang instrumen pemantauan
   4.3 Objektif dalam meninjau instrumen pemantauan

5. Aspek kritis
   5.1 Ketepatan dalam memilih instrumen pemantauan sesuai Kebutuhan Keamanan Informasi

BAB III
PENUTUP

Dengan ditetapkannya Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan Yang Berhubungan Dengan Itu (YBDI) Bidang Keamanan Informasi, maka SKKNI ini menjadi acuan dalam penyusunan jenjang kualifikasi nasional, penyelenggaraan pendidikan, pelatihan, dan sertifikasi kompetensi.

MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA,

IDA FAUZIYAH