MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA

KEPUTUSAN MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA

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

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI KETENAGAKERJAAN REPUBLIK INDONESIA,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 26 Peraturan Menteri Tenaga Kerja dan Transmigrasi Nomor 8 Tahun 2012 tentang Tata Cara Penetapan Standar Kompetensi Kerja Nasional Indonesia, perlu menetapkan Keputusan Menteri tentang Penetapan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Kegiatan Pemrograman, Konsultasi Komputer dan Kegiatan 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. Keputusan Presiden Nomor 121/P Tahun 2014;

5. Peraturan Menteri Tenaga Kerja dan Transmigrasi Nomor 8 Tahun 2012 tentang Tata Cara Penetapan Standar Kompetensi Kerja Nasional Indonesia (Berita Negara Republik Indonesia Tahun 2012 Nomor 364);

Memperhatikan :

1. Hasil Konvensi Nasional Rancangan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Kegiatan Pemrograman, Konsultasi Komputer dan Kegiatan ybdi Bidang Keamanan Informasi yang diselenggarakan tahun 2011 bertempat di Jakarta;

2. Surat Kepala Puslitbang Literasi dan Profesi SDM Kominfo Nomor B-526/KOMINFO/BLSDM.5/LT.03.07/12/2014 tanggal 19 Desember 2014 perihal Pengajuan RSKKNI menjadi SKKNI;

MEMUTUSKAN:

Menetapkan :

KESATU : Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Kegiatan Pemrograman, Konsultasi Komputer dan Kegiatan ybdi Bidang Keamanan Informasi, sebagaimana tercantum dalam Lampiran dan merupakan bagian yang tidak terpisahkan dari Keputusan Menteri ini.

KEDUA : Standar Kompetensi Kerja Nasional Indonesia sebagaimana dimaksud dalam Diktum KESATU berlaku secara nasional dan menjadi acuan penyelenggaraan pendidikan dan pelatihan profesi, uji kompetensi dan sertifikasi profesi.

KETIGA : Standar Kompetensi Kerja Nasional Indonesia sebagaimana dimaksud dalam Diktum KESATU pemberlakuannya ditetapkan oleh Menteri Komunikasi dan Informatika.

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

KELIMA : Keputusan Menteri ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 24 Februari 2015

MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA,

KETENAGAKERJAAN R.I. MENTERI

M. HANIF DHAKIRI

LAMPIRAN
KEPUTUSAN MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA

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

BAB I
PENDAHULUAN

A. Latar Belakang

Selama beberapa dekade terakhir, evolusi teknologi yang cepat telah turut pula mempercepat transformasi masyarakat terhadap budaya digital. Kecepatan perubahan ini telah menyebabkan perbedaan dalam komposisi teknologi informasi dan komunikasi (TIK) khususnya tenaga kerja keamanan teknologi informasi (TI). Variasi dalam pelatihan, keahlian, dan pengalaman merupakan konsekuensi wajar dari evolusi ini, dan tercermin dalam semakin melimpahnya kegiatan perekrutan, pendidikan, dan praktek retensi antara organisasi/perusahaan. Dari awal revolusi digital, organisasi publik, swasta, dan akademis memiliki semua sumber daya yang berdedikasi untuk mengembangkan bidang keamanan TI praktis dan telah membuat kemajuan yang signifikan.

Hal ini semakin penting untuk profesional/tenaga kerja bidang teknologi informasi dan komunikasi, khususnya sub-bidang keamanan TI untuk memenuhi tantangan hari ini, dan secara proaktif menggapai tujuan mereka di masa depan. Keterbukaan dan kuantitas sistem terhubung ke Internet, konvergensi sistem gambar, suara dan komunikasi data, ketergantungan organisasi terhadap sistem tersebut dan ancaman yang muncul dari lawan canggih dan orang-orang yang tidak bertanggungjawab yang berusaha untuk ‘mengganggu’ sistem itu menggarisbawahi kebutuhan spesialis keamanan TI yang terlatih dan memiliki perangkat yang mencukup (*well-equipped*). Pelayanan bersama infrastruktur serta informasi antara pemerintah dan industri

menunjukkan perlunya model inovatif peran, tanggung jawab, dan kompetensi yang dibutuhkan untuk tenaga kerja bidang teknologi informasi dan komunikasi khususnya sub-bidang keamanan TI.

Untuk membantu organisasi dan anggota saat ini dan masa depan tenaga kerja ini, Kementerian Komunikasi dan Informatika (KemKominfo) bekerja dengan para ahli dari akademisi, pemerintah, dan sektor swasta mengembangkan sebuah kerangka tingkat tinggi yang menetapkan standar nasional mewakili pengetahuan dan keterampilan penting yang harus dimiliki oleh praktisi keamanan TI.

Atas dasar pertimbangan tersebut diatas, KemKominfo mendorong upaya-upaya yang diperlukan untuk membangun dasar bagi pengembangan program sertifikasi keamanan yang akan diterima secara luas oleh sektor publik dan swasta. Kementerian Kominfo, Kementerian Tenaga Kerja dan lembaga pemerintah lainnya dapat membantu upaya-upaya ini dengan efektif mengartikulasikan kebutuhan masyarakat keamanan TI. Sebagai tindak lanjut dari upaya ini adalah program Pelatihan dan Pendidikan di bidang teknologi informasi dan komunikasi sub-bidang keamanan TI untuk pembangunan angkatan kerja yang dapat mencukupi kebutuhan industri nasional.

Sebagai acuan maka dibutuhkan sebuah kerangka standar bidang keamanan informasi yang menitikberatkan kepada kompetensi yang harus dimiliki oleh tiap individu yang melakukan fungsi-fungsi keamanan informasi. Atas dasar kebutuhan inilah disusun Standar Kompetensi Kerja Nasional Indonesia (SKKNI) bidang Teknologi Informasi dan Komunikasi sub-bidang Keamanan Informasi.

SKKNI bidang Teknologi Informasi dan Komunikasi sub-bidang Keamanan Informasi digunakan untuk memberikan panduan untuk identifikasi dan kategorisasi posisi dan sertifikasi personil yang melakukan fungsi keamanan informasi yang mendukung implementasi keamanan informasi organisasi. Tenaga kerja bidang keamanan informasi termasuk, namun tidak terbatas pada, semua individu melakukan salah satu fungsi keamanan informasi dalam organisasi sesuai dengan kebijakan, prosedur dan peraturan yang berlaku.

Standar ini dirumuskan dengan menggunakan acuan sebagai berikut.

3.1 Undang-Undang Nomor 13 Tahun 2003 tentang Ketenagakerjaan;

3.2 Peraturan Pemerintah Nomor 23 Tahun 2004 tentang Badan Nasional Sertifikasi Profesi;

3.3 Peraturan Menteri Tenaga Kerja dan Transmigrasi Nomor 5 Tahun 2012 tentang Sistem Standarisasi Kompetensi Kerja Nasional;

3.4 Peraturan Menteri Tenaga Kerja dan Transmigrasi Nomor 8 Tahun 2012 tentang Tata Cara Penetapan Standar Kompetensi Kerja Nasional Indonesia;

3.5 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;

3.6 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik.

Penyusunan Standar Kompetensi Kerja Nasional Indonesia Bidang Teknologi Informasi dan Komputer Subbidang Keamanan Informasi mempunyai tujuan sebagai berikut:

1. Menetapkan dasar (*baseline*) keterampilan teknis dan manajemen keamanan informasi di antara SDM yang melaksanakan fungsi keamanan informasi dalam organisasi.
2. Mengembangkan dan meremajakan keterampilan secara formal untuk tenaga kerja bidang keamanan informasi yang terdiri dari beragam model pelatihan, program magang (*on-the-job training*), praktek-praktek dan sertifikasi/re-sertifikasi.
3. Verifikasi pengetahuan dan keterampilan tenaga kerja bidang keamanan informasi melalui pengujian sertifikasi standar.

B. Pengertian

1. Pengertian Keamanan Informasi

   Berdasarkan *SANS Institute Information Security Resources*, keamanan Informasi mengacu pada proses dan metodologi yang dirancang dan dilaksanakan untuk melindungi cetak, elektronik, atau bentuk lain dari informasi rahasia, pribadi dan sensitif atau

data dari akses yang tidak sah, penggunaan, penyalahgunaan, pengungkapan, kehancuran, modifikasi, atau gangguan.

2. Pengertian Perlindungan Informasi

   Berdasarkan pasal 26 ayat 1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang menyatakan bahwa “kecuali ditentukan oleh Peraturan Perundang-undangan, penggunaan, setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan”.

3. Manajemen Risiko Keamanan Informasi

   Menurut ISO/IEC 27001 dan ISO/IEC 27002, istilah risiko keamanan informasi adalah potensi ancaman yang ada akan mengeksploitasi kerentanan aset atau kelompok aset sehingga dapat menyebabkan kerugian pada suatu organisasi. Berdasarkan hal ini maka ISO/IEC 27005 menyadari perlunya manajemen risiko keamanan informasi untuk mengidentifikasi kebutuhan organisasi mengenai persyaratan keamanan informasi dan menciptakan sistem manajemen keamanan informasi yang efektif. Pendekatan ini secara umum harus sesuai untuk lingkungan organisasi dan secara khusus harus diselaraskan dengan manajemen risiko organisasi secara keseluruhan. Upaya keamanan harus menangani risiko secara efektif dan tepat waktu dimanapun dan kapanpun dibutuhkan.

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 rekruitmen.
   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

Tabel1. Susunan komite standar kompetensi RSKKNI Sektor Keamanan Informasi

NO	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Kepala Balitbang SDM	Kementerian Kominfo	Pengarah
2.	Ka. Puslitbang Literasi dan Profesi Kominfo	Kementerian Kominfo	Penanggung Jawab
3.	Sekretaris Badan Litbang SDM	Kementerian Kominfo	Ketua Pelaksana
4.	Kepala Biro Perencanaan	Kementerian Kominfo	Wakil Ketua Pelaksana
5.	Sekretaris Ditjen Aplikasi Informatika	Kementerian Kominfo	Sekretaris
6.	Sekretaris Ditjen Informasi dan Komunikasi Publik	Kementerian Kominfo	Anggota
7.	Sekretaris Ditjen Penyelenggaraan Pos dan Informatika	Kementerian Kominfo	Anggota
8.	Ketua Umum Ikatan Profesi Komputer dan Informatika Indonesia	IPKIN	Anggota

Tabel 2. Susunan tim perumus RSKKNI

NO	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Didik Partono Rudiarto	Direktur Inixindo	Anggota
2.	Carlia Wisaksono	Pengurus APTIKOM	Anggota
3.	Hogan Kusnadi	Presiden Direktur UniPro	Anggota
4.	Gildas Deograt Lumy	Koordinator KKI	Anggota
5.	Bysiron Wahyudi	Koordinator Operasi ID-SIRTII	Anggota
6.	Andika Triwidada	ID-CERT	Anggota
7.	Tin Tin Hadijanto	Country Representative ECCouncil	Anggota
8.	Arief Wibowo	Wakil Dekan Akademik FTI Universitas Budiluhur	Anggota
9.	Muhammad Ainur Rony	Kaprodi TI Universitas Budiluhur	Anggota
10.	Imelda	Dosen Univ. Budiluhur	Anggota

Tabel 3. Susunan Tim verifikator RSKKNI

NO	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Kepala Balitbang SDM	Kementerian Kominfo	Pengarah
2.	Kapuslitbang Literasi dan Profesi	Kementerian Kominfo	Penanggung Jawab
3.	Anny Triana	Kementerian Kominfo	Ketua Pelaksana
4.	Aldhino Anggorosesar	Kementerian Kominfo	Wakil Ketua Pelaksana
5.	Ika Deasy Ariyani	Kementerian Kominfo	Sekretaris
6.	Desy Bintaria	Kementerian Kominfo	Anggota
7.	Bambang Hariyadi	Kementerian Kominfo	Anggota
8.	Fajar Rulhudana	Kementerian Kominfo	Anggota

BAB II

STANDAR KOMPETENSI KERJA NASIONAL INDONESIA

A. Pemetaan Kompetensi

Tabel 4. Pemetaan SKKNI Bidang Keamanan Informasi

TUJUAN UTAMA	FUNGSI KUNCI	FUNGSI UTAMA	FUNGSI DASAR
Mengelola sistem informasi yang aman dan akuntabel berdasarkan aturan dan kebijakan yang berlaku	Menerapkan prinsip keamanan informasi	Menerapkan prinsip perlindungan informasi	1. Menerapkan prinsip perlindungan informasi 2. Menyelaraskan penerapan prinsip perlindungan informasi dengan misi dan tujuan organisasi
		Menerapkan prinsip keamanan informasi	3. Menerapkan prinsip keamanan informasi untuk penggunaan jaringan internet 4. Menerapkan prinsip keamanan informasi pada transaksi elektronik
	Mengelola kebijakan, regulasi dan prosedur keamanan informasi	Mengelola kebijakan keamanan informasi	5. Menyusun dokumen kebijakan keamanan informasi 6. Melaksanakan kebijakan keamanan informasi 7. Mengelola siklus informasi (klasifikasi, kategorisasi, penanggung-jawab) 8. Melaksanakan ketentuan hukum yang berlaku tentang keamanan informasi
		Menyusun dan melaksanakan prosedur keamanan informasi	9. Mengelola prosedur keamanan informasi 10. Mengimplementasikan prosedur keamanan informasi dalam kegiatan pengadaan

TUJUAN UTAMA	FUNGSI KUNCI	FUNGSI UTAMA	FUNGSI DASAR
	Melaksanakan tata kelola, manajemen risiko dan audit keamanan informasi	Menerapkan tata kelola keamanan informasi	11. Menerapkan standar-standar keamanan informasi yang berlaku 12. Mengaplikasikan ketentuan/persyaratan keamanan informasi 13. Mengelola proses sertifikasi dan akreditasi untuk keamanan informasi
		Mengelola sdm dan organisasi keamanan informasi	14. Melaksanakan alokasi pemisahan tugas-tugas 15. Melaksanakan koordinasi dan pengarahan pelaksanaan tugas-tugas keamanan informasi 16. Mengelola sdm yang terkait dengan tugas-tugas keamanan informasi 17. Mengelola program peningkatan kepedulian dan pelatihan terkait dengan keamanan informasi
		Mengelola risiko keamanan informasi	18. Mengelola risiko keamanan informasi 19. Melakukan kajian keamanan informasi 20. Mengelola *log*
		Melaksanakan audit keamananan informasi	21. Mengelola audit keamanan informasi 22. Melakukan evaluasi kinerja keamanan informasi
	Mengelola arsitektur keamanan informasi	Menerapkan keamanan fisik dan lingkungan	23. Mengelola keamanan fisik 24. Melaksanakan pencatatan asset

TUJUAN UTAMA	FUNGSI KUNCI	FUNGSI UTAMA	FUNGSI DASAR
		Mengelola keamanan infrastuktur	25. Mengelola sistem pertahanan dan perlindungan keamanan informasi 26. Menyediakan dukungan keamanan bagi pengguna 27. Mengimplementasikan konfigurasi keamanan informasi 28. Mengelola *script* keamanan informasi 29. Mengelola perimeter keamanan
		Mengelola keamanan aplikasi dan piranti lunak	30. Melakukan instalasi piranti lunak 31. Mengelola aspek keamanan sistem informasi pada setiap kegiatan *upgrade*/peremajaan sistem informasi
	Menerapkan kontrol akses	Menyiapkan kontrol akses	32. Menerapkan kontrol akses berdasarkan konsep/metodologi yang telah ditetapkan 33. Mengidentifikasi serangan-serangan terhadap kontrol akses
		Mengelola kontrol akses	34. Mengkaji efektivitas penerapan kontrol akses 35. Mengelola siklus pemberian akses
	Melaksanakan analisa intrusi dan uji penetrasi	Melaksanakan analisa intrusi	36. Melaksanakan uji coba sistem pertahanan keamanan informasi 37. Mendeteksi kerentanan (vulnerabilitas) keamanan dan potensi pelanggaran
		Melaksanakan uji penetrasi	38. Melaksanakan evaluasi kelemahan (vulnerabilitas) keamanan 39. Mengimplementasikan koreksi atas kerentanan keamanan informasi

TUJUAN UTAMA	FUNGSI KUNCI	FUNGSI UTAMA	FUNGSI DASAR
	Mengelola penanganan insiden	Menerapkan penanganan insiden	40. Mengelola insiden keamanan informasi 41. Menyediakan dukungan keamanan untuk permasalahan perangkat keras dan piranti lunak 42. Melakukan aktifitas penghapusan hak akses
		Melaksanakan manajemen perbaikan	43. Mengimplementasikan manajemen perbaikan/respon yang terkait dengan keamanan informasi 44. Mengaplikasikan *patch* keamanan
	Mengelola pemulihan bencana dan manajemen kelangsungan usaha	Menerapkan integritas informasi	45. Mengelola integritas informasi 46. Mengelola penggunakan media penyimpanan sementara (*removable media*)
		Mengelola pemulihan bencana	47. Merancang dan mengelola sistem *backup* 48. Melaksanakan kegiatan pemulihan data

B. Daftar Unit Kompetensi

NO	KODE UNIT	JUDUL UNIT KOMPETENSI
1.	J.62090.001.01	Menerapkan Prinsip Perlindungan Informasi
2.	J.62090.002.01	Menyelaraskan Penerapan Prinsip Perlindungan Informasi dengan Misi dan Tujuan Organisasi
3.	J.62090.003.01	Menerapkan Prinsip Keamanan Informasi untuk Penggunaan Jaringan Internet
4.	J.62090.004.01	Menerapkan Prinsip Keamanan Informasi pada Transaksi Elektronik
5.	J.62090.005.01	Menyusun Dokumen Kebijakan Keamanan Informasi
6.	J.62090.006.01	Melaksanakan Kebijakan Keamanan Informasi
7.	J.62090.007.01	Mengelola Siklus Informasi (Klasifikasi, Kategorisasi, Penanggung-Jawab)
8.	J.62090.008.01	Melaksanakan Ketentuan Hukum yang Berlaku tentang Keamanan Informasi

NO	KODE UNIT	JUDUL UNIT KOMPETENSI
9.	J.62090.009.01	Mengelola Prosedur Keamanan Informasi
10.	J.62090.010.01	Mengimplementasikan Prosedur Keamanan Informasi Dalam Kegiatan Pengadaan
11.	J.62090.011.01	Menerapkan Standar-Standar Keamanan Informasi yang Berlaku
12.	J.62090.012.01	Mengaplikasikan Ketentuan/Persyaratan Keamanan Informasi
13.	J.62090.013.01	Mengelola Proses Sertifikasi dan Akreditasi untuk Keamanan Informasi
14.	J.62090.014.01	Melaksanakan Alokasi Pemisahan Tugas-Tugas
15.	J.62090.015.01	Melaksanakan Koordinasi dan Pengarahan Pelaksanaan Tugas-Tugas Keamanan Informasi
16.	J.62090.016.01	Mengelola Sdm yang Terkait dengan Tugas-Tugas Keamanan Informasi
17.	J.62090.017.01	Mengelola Program Peningkatan Kepedulian dan Pelatihan Terkait dengan Keamanan Informasi
18.	J.62090.018.01	Mengelola Risiko Keamanan Informasi
19.	J.62090.019.01	Melakukan Kajian Keamanan Informasi
20.	J.62090.020.01	Mengelola *Log*
21.	J.62090.021.01	Mengelola Audit Keamanan Informasi
22.	J.62090.022.01	Melakukan Evaluasi Kinerja Keamanan Informasi
23.	J.62090.023.01	Mengelola Keamanan Fisik
24.	J.62090.024.01	Melaksanakan Pencatatan *Asset*
25.	J.62090.025.01	Mengelola Sistem Pertahanan dan Perlindungan Keamanan Informasi
26.	J.62090.026.01	Menyediakan Dukungan Keamanan Bagi Pengguna
27.	J.62090.027.01	Mengimplementasikan Konfigurasi Keamanan Informasi
28.	J.62090.028.01	Mengelola *Script* Keamanan Informasi
29.	J.62090.029.01	Mengelola Perimeter Keamanan
30.	J.62090.030.01	Melakukan Instalasi Piranti Lunak

NO	KODE UNIT	JUDUL UNIT KOMPETENSI
31.	J.62090.031.01	Mengelola Aspek Keamanan Sistem Informasi pada Setiap Kegiatan *Upgrade*/Peremajaan Sistem Informasi
32.	J.62090.032.01	Menerapkan Kontrol Akses Berdasarkan Konsep/Metodologi yang Telah Ditetapkan
33.	J.62090.033.01	Mengidentifikasi Serangan-Serangan Terhadap Kontrol Akses
34.	J.62090.034.01	Mengkaji Efektivitas Penerapan Kontrol Akses
35.	J.62090.035.01	Mengelola Siklus Pemberian Akses
36.	J.62090.036.01	Melaksanakan Uji Coba Sistem Pertahanan Keamanan Informasi
37.	J.62090.037.01	Mendeteksi Kerentanan (Vulnerabilitas) Keamanan dan Potensi Pelanggaran
38.	J.62090.038.01	Melaksanakan Evaluasi Kelemahan (Vulnerabilitas) Keamanan
39.	J.62090.039.01	Mengimplementasikan Koreksi Atas Kerentanan Keamanan Informasi
40.	J.62090.040.01	Mengelola Insiden Keamanan Informasi
41.	J.62090.041.01	Menyediakan Dukungan Keamanan Untuk Permasalahan Perangkat Keras dan Piranti Lunak
42.	J.62090.042.01	Melakukan Aktifitas Penghapusan Hak Akses
43.	J.62090.043.01	Mengimplementasikan Manajemen Perbaikan/Respon yang Terkait dengan Keamanan Informasi
44.	J.62090.044.01	Mengaplikasikan *Patch* Keamanan
45.	J.62090.045.01	Mengelola Integritas Informasi
46.	J.62090.046.01	Mengelola Penggunakan Media Penyimpanan Sementara (*Removable Media*)
47.	J.62090.047.01	Merancang dan Mengelola Sistem *Backup*
48.	J.62090.048.01	Melaksanakan Kegiatan Pemulihan Data

C. Uraian Unit Kompetensi

KODE UNIT : **J.62090.001.01**

JUDUL UNIT : **Menerapkan Prinsip Perlindungan Informasi**

DESKRIPSI UNIT : Melaksanakan kebijakan dan prosedur keamanan informasi yang telah ditetapkan untuk melindungi informasi terkait dengan interkoneksi sistem informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mendefinisikan prosedur keamanan informasi yang tepat untuk tiap klasifikasi	1.1 Prosedur penamaan yang mencakup informasi dalam format elektronik maupun fisik didokumentasikan sesuai dengan klasifikasi yang telah ditetapkan. 1.2 Persyaratan keamanan bagi masing-masing klasifikasi label diidentifikasi 1.3 Prosedur pemrosesan, penyimpanan, pengiriman dan penghapusan sesuai persyaratan keamanan didefinisikan. 1.4 Prosedur penjagaan dan pencatatan ketika terjadi *event* yang terkait dengan keamanan pada masing-masing klasifikasi didefinisikan.
2. Mengidentifikasi kelemahan dari informasi dalam sistem komunikasi bisnis	2.1 Prosedur dan kebijakan yang terkait dengan sistem komunikasi bisnis diidentifikasi. 2.2 Kelemahan dari informasi diidentifikasi, dianalisa dan dievaluasi. 2.3 Solusi pemecahan terhadap masalah kelemahan dalam sistem komunikasi bisnis ditetapkan.
3. Menerapkan akses kontrol lingkungan Komputasi yang sesuai	3.1 Sistem dan prosedur akses kontrol yang telah ditetapkan dideskripsikan. 3.2 *Log* untuk setiap kegiatan akses secara rinci dibuat.
4. Mematuhi dan melaksanakan petunjuk yang terdapat pada dokumen yang diterbitkan khusus oleh pemerintah atau badan-badan resmi terkait untuk mengelola sistem operasi	4.1 Dokumen yang diterbitkan khusus oleh pemerintah atau badan-badan resmi terkait untuk mengelola sistem operasi lingkungan komputasi diarsipkan. 4.2 Butir-butir pokok yang terdapat pada dokumentasi tersebut diatas dideskripsikan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
5. Mengumpulkan dan memelihara data yang diperlukan untuk memenuhi persyaratan pelaporan keamanan sistem	5.1 Data yang diperlukan untuk memenuhi persyaratan pelaporan keamanan sistem dideskripsikan. 5.2 Laporan berkala keamanan sistem dibuat.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan
   - 2.1 Peralatan

     (Tidak ada.)
   - 2.2 Perlengkapan

     (Tidak ada.)

3. Peraturan yang diperlukan
   - 3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   - 3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   - 4.1 Norma

     (Tidak ada.)
   - 4.2 Standar

     4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam melaksanakan kebijakan dan prosedur keamanan informasi yang telah ditetapkan untuk melindungi informasi terkait dengan interkoneksi sistem informasi. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

   3.1 Pengetahuan

      3.1.1 Standar yang berlaku terkait dengan keamanan informasi

      3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

      3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall*, IPS)

      3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

   3.2 Keterampilan

      3.2.1 Mengoperasikan perangkat keras dan piranti lunak

      3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem

      3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan
   4.1 Disiplin
   4.2 Teliti
   4.3 Tanggung jawab

5. Aspek kritis
   5.1 Ketepatan dalam menentukan prosedur penamaan yang mencakup informasi dalam format elektronik maupun fisik didokumentasikan sesuai dengan klasifikasi yang telah ditetapkan
   5.2 Ketepatan dalam mengidentifikasi prosedur dan kebijakan yang terkait dengan sistem komunikasi bisnis
   5.3 Ketepatan dalam mendeskripsikan sistem dan prosedur akses kontrol yang telah ditetapkan
   5.4 Ketepatan dalam membuat *log* untuk setiap kegiatan akses secara rinci
   5.5 Ketepatan dalam mendeskripsikan data yang diperlukan untuk memenuhi persyaratan pelaporan keamanan sistem
   5.6 Ketepatan dalam membuat laporan berkala keamanan sistem

KODE UNIT : **J.62090.002.01**

JUDUL UNIT : **Menyelaraskan Penerapan Prinsip Perlindungan Informasi dengan Misi dan Tujuan Organisasi**

DESKRIPSI : Melihat sejauh mana kesesuaian prinsip perlindungan informasi dengan misi dan tujuan organisasi yang sudah dilakukan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi kesesuaian prosedur keamanan informasi yang tepat untuk tiap klasifikasi dengan misi dan tujuan organisasi	1.1 Kesesuaian prosedur penamaan yang mencakup informasi dalam format elektronik maupun fisik didokumentasikan sesuai dengan klasifikasi yang telah ditetapkan dengan misi dan tujuan organisasi diidentifikasi. 1.2 Kesesuaian persyaratan keamanan bagi masing-masing klasifikasi label diidentifikasi dengan misi dan tujuan organisasi diidentifikasi. 1.3 Kesesuaian prosedur pemrosesan, penyimpanan, pengiriman dan penghapusan sesuai persyaratan keamanan didefinisikan dengan misi dan tujuan organisasi diidentifikasi. 1.4 Kesesuaian prosedur penjagaan dan pencatatan ketika terjadi *event* yang terkait dengan keamanan pada masing-masing klasifikasi didefinisikan dengan misi dan tujuan organisasi diidentifikasi.
2. Mengidentifikasi kelemahan dari informasi dalam sistem komunikasi bisnis	2.1 Kesesuaian prosedur dan kebijakan yang terkait dengan sistem komunikasi bisnis diidentifikasi dengan misi dan tujuan organisasi diidentifikasi. 2.2 Kesesuaian kelemahan dari informasi diidentifikasi, dianalisa dan dievaluasi dengan misi dan tujuan organisasi diidentifikasi. 2.3 Kesesuaian solusi pemecahan terhadap masalah kelemahan dalam sistem komunikasi bisnis ditetapkan dengan misi dan tujuan organisasi diidentifikasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
3. Menerapkan akses kontrol lingkungan komputasi yang sesuai	3.1 Kesesuaian sistem dan prosedur akses kontrol yang telah ditetapkan dideskripsikan dengan misi dan tujuan organisasi diidentifikasi. 3.2 Kesesuaian *log* untuk setiap kegiatan akses secara rinci dibuat dengan misi dan tujuan organisasi diidentifikasi.
4. Mengidentifikasi kesesuaian dalam mematuhi dan melaksanakan petunjuk yang terdapat pada dokumen yang diterbitkan khusus oleh pemerintah atau badan-badan resmi terkait untuk mengelola sistem operasi agar misi dan tujuan organisasi terwujud	4.1 Kesesuaian dokumen yang diterbitkan khusus oleh pemerintah atau badan-badan resmi terkait untuk mengelola sistem operasi lingkungan komputasi diarsipkan dengan misi dan tujuan organisasi diidentifikasi. 4.2 Kesesuaian butir-butir pokok yang terdapat pada dokumentasi tersebut diatas dideskripsikan dengan misi dan tujuan organisasi diidentifikasi
5. Mengidentifikasi kesesuaian pengumpulan dan pemeliharaan data yang diperlukan untuk memenuhi persyaratan pelaporan keamanan sistem agar misi dan tujuan organisasi terwujud	5.1 Kesesuaian data yang diperlukan untuk memenuhi persyaratan pelaporan keamanan sistem dideskripsikan dengan misi dan tujuan organisasi diidentifikasi. 5.2 Kesesuaian laporan berkala keamanan sistem dibuat dengan misi dan tujuan organisasi diidentifikasi.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

   2.2 Perlengkapan

   (Tidak ada.)

3. Peraturan yang diperlukan

   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar

   4.1 Norma

   (Tidak ada.)

   4.2 Standar

   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam melihat sejauh mana kesesuaian prinsip perlindungan informasi dengan misi dan tujuan organisasi yang sudah dilakukan. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
    3.1 Pengetahuan
        3.1.1 Standar yang berlaku terkait dengan keamanan informasi
        3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)
        3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall*, IPS)
        3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)
    3.2 Keterampilan
        3.2.1 Mengoperasikan perangkat keras dan piranti lunak
        3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi
        3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan
    4.1 Disiplin
    4.2 Teliti
    4.3 Tanggung jawab

5. Aspek kritis
    5.1 Ketepatan dalam mengidentifikasi kesesuaian persyaratan keamanan bagi masing-masing klasifikasi label diidentifikasi dengan misi dan tujuan organisasi.
    5.2 Ketepatan dalam mengidentifikasi kesesuaian persyaratan keamanan bagi masing-masing klasifikasi label diidentifikasi dengan misi dan tujuan organisasi.
    5.3 Ketepatan dalam mengidentifikasi kesesuaian solusi pemecahan terhadap masalah kelemahan dalam sistem komunikasi bisnis ditetapkan dengan misi dan tujuan organisasi

KODE UNIT : **J.62090.003.01**

JUDUL UNIT : **Menerapkan Prinsip Keamanan Informasi untuk Penggunaan Jaringan Internet**

DESKRIPSI : Menerapkan prinsip keamanan informasi yang terkait penggunaan jaringan internet agar terlindungi sehingga meminimalkan risiko-risiko keamanan informasi yang dapat terjadi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mematuhi dan menerapkan kebijakan dan prosedur keamanan informasi yang terkait dengan penggunaan jaringan internet	1.1 Kebijakan, prasyarat dan prosedur keamanan yang terkait penggunaan jaringan internet di identifikasi. 1.2 Laporan anomali pada penggunaan jaringan internet dibuat.
2. Mengidentifikasi tipe kelemahan dan jenis-jenis serangan dalam jaringan internet	2.1 Dokumen tentang tipe-tipe kelemahan dan jenis-jenis serangan diidentifikasi. 2.2 Jenis serangan melalui *e-mail* diidentifikasi. 2.3 Jenis serangan virus dan dampaknya diidentifikasi. 2.4 Jenis serangan *worm* dan *botnet* dan dampaknya diidentifikasi.
3. Mengaplikasikan penggunaan jaringan internet secara aman	3.1 Piranti lunak untuk keamanan penggunaan jaringan internet dipergunakan. 3.2 Cara-cara menggunakan *e-mail* secara aman dipelajari. 3.3 Cara-cara menjelajah internet menggunakan *browser* secara aman dipelajari. 3.4 Cara-cara menangkal virus menggunakan piranti lunak anti virus didefinisikan.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan

fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan
   2.1 Peralatan
   (Tidak ada.)
   2.2 Perlengkapan
   (Tidak ada.)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian
   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam menerapkan prinsip keamanan informasi yang terkait penggunaan jaringan internet agar terlindungi sehingga meminimalkan risiko-risiko keamanan informasi yang dapat terjadi. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:
   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.
   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.
   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Standar yang berlaku terkait dengan keamanan informasi

3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall*, IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam mengidentifikasi kebijakan, prasyarat dan prosedur keamanan yang terkait penggunaan jaringan internet

5.2 Ketepatan dalam membuat laporan anomali pada penggunaan jaringan internet

KODE UNIT : **J.62090.004.01**

JUDUL UNIT : **Menerapkan Prinsip Keamanan Informasi pada Transaksi Elektronik**

DESKRIPSI : Menerapkan prinsip keamanan informasi yang terkait dalam transaksi elektronik agar terlindungi sehingga dapat mencegah pengiriman tidak lengkap, salah alamat, pengubahan pesan tanpa otorisasi, penyingkapan tanpa otorisasi, duplikasi atau penjawaban pesan tanpa otorisasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasikan dan memenuhi kebutuhan terkait kerahasiaan, integritas, bukti dari pengguna dokumen kunci dan kontrak yang diakui	1.1 Kebijakan, prasyarat dan prosedur keamanan yang terkait diterapkan dalam konfigurasi sistem operasi, insfrastruktur teknologi informasi, perangkat dan aplikasi diidentifikasi. 1.2 Laporan kegiatan transaksi elektronik bagi pengguna akhir dibuat.
2. Menetapkan aspek-aspek transaksi	2.1 Bukti keabsahan elektronik (*signature*) oleh semua pihak yang terlibat dalam suatu transaksi ditetapkan. 2.2 Enkripsi terhadap jalur komunikasi antara pihak-pihak yang terlibat diaplikasikan. 2.3 Protokol keamanan yang digunakan untuk komunikasi antara pihak-pihak yang terlibat dievaluasi 2.4 Integrasi dan penggabungan keamanan terkait semua proses transaksi yang dilakukan diterapkan.
3. Melaksanakan dan memantau perlindungan keamanan untuk sistem infrastruktur dan penggunaan teknologi informasi sesuai dengan rencana implementasi dan prosedur operasi standar	3.1 Laporan pelaksanaan hasil pemantauan perlindungan keamanan sistem infrastruktur dibuat. 3.2 *Log audit* hasil pemantauan perlindungan keamanan atas prosedur operasi standar dibuat.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

   2.2 Perlengkapan

   (Tidak ada.)

3. Peraturan yang diperlukan

   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar

   4.1 Norma

   (Tidak ada.)

   4.2 Standar

   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam menerapkan prinsip keamanan informasi yang terkait dalam transaksi elektronik agar terlindungi sehingga dapat mencegah pengiriman tidak lengkap, salah alamat, pengubahan pesan tanpa otorisasi, penyingkapan

tanpa otorisasi, duplikasi atau penjawaban pesan tanpa otorisasi. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Standar yang berlaku terkait dengan keamanan informasi

3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall*, IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam mengidentifikasi kebijakan, prasyarat dan prosedur keamanan yang terkait diterapkan dalam konfigurasi sistem operasi, insfrastruktur teknologi informasi, perangkat dan aplikasi

5.2 Ketepatan dalam membuat laporan kegiatan transaksi elektronik bagi pengguna akhir

5.3 Ketepatan dalam menetapkan bukti keabsahan elektronik (*signature*) oleh semua pihak yang terlibat dalam suatu transaksi

5.4 Ketepatan dalam membuat laporan pelaksanaan hasil pemantauan perlindungan keamanan sistem infrastruktur

5.5 Ketepatan dalam membuat *log audit* hasil pemantauan perlindungan keamanan atas prosedur operasi standar

KODE UNIT : **J.62090.005.01**

JUDUL UNIT : **Menyusun Dokumen Kebijakan Keamanan Informasi**

DESKRIPSI : Menyusun dan menetapkan dokumen kebijakan keamanan informasi yang diotorisasi oleh pihak manajemen untuk selanjutnya dipublikasikan dan dikomunikasikan kepada seluruh pegawai dan pihak-pihat terkait lain.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi alternatif strategi keamanan fungsional untuk mengatasi masalah keamanan dilingkungan jaringan sistem informasi organisasi	1.1 Daftar alternatif strategi keamanan fungsional untuk mengatasi masalah keamanan dilingkungan jaringan sistem informasi organisasi disusun. 1.2 Prioritas penerapan alternatif strategi keamanan fungsional untuk mengatasi masalah keamanan dilingkungan jaringan sistem informasi organisasi disetujui oleh pimpinan organisasi.
2. Menganalisis strategi keamanan yang telah diidentifikasi dan memilih pendekatan yang terbaik atau *best practice* untuk tingkatan strategis	2.1 Referensi *best practice* untuk penerapan strategi keamanan pada tingkatan strategis diidentifikasi. 2.2 Rekomendasi hasil analisis strategi keamanan yang sesuai untuk tingkatan strategis dibuat.
3. Mengevaluasi usulan-usulan solusi keamanan untuk menentukan apakah solusi tersebut tepat secara efektif untuk kebutuhan strategis organisasi	3.1 Daftar usulan-usulan solusi keamanan untuk kebutuhan strategis organisasi disusun. 3.2 Rekomendasi hasil analisa usulan-usulan solusi keamanan untuk kebutuhan strategis organisasi dibuat.
4. Melakukan evaluasi biaya manfaat, analisis ekonomi dan analisis risiko dalam proses pengambilan keputusan	4.1 Laporan hasil evaluasi biaya manfaat dibuat. 4.2 Laporan hasil analisis ekonomi dibuat. 4.3 Laporan hasil analisis risiko dibuat.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
5. Menetapkan tanggung jawab dan akuntabilitas informasi untuk setiap Sistem Informasi organisasi dan menerapkan skema akses berbasis peran/tanggung jawab/jabatan	5.1 Daftar rincian pekerjaan untuk setiap peran/jabatan dalam organisasi dan akuntabilitas informasi untuk masing-masing peran/jabatan tersebut disusun. 5.2 Tugas dan tanggung jawab yang terkait dengan keamanan sistem informasi diaplikasikan.
6. Menganalisis, mengembangkan, menyetujui, dan mengeluarkan kebijakan Keamanan dalam tingkatan strategis	6.1 Daftar risiko sistem informasi, analisa dampak bisnis dan rencana mitigasi disusun. 6.2 Kebijakan keamanan informasi dalam tingkatan strategis tersusun.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan
   - 2.1 Peralatan

     (Tidak ada.)
   - 2.2 Perlengkapan

     (Tidak ada.)

3. Peraturan yang diperlukan
   - 3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   - 3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam menyusun dan menetapkan dokumen kebijakan keamanan informasi yang diotorisasi oleh pihak manajemen untuk selanjutnya dipublikasikan dan dikomunikasikan kepada seluruh pegawai dan pihak-pihat terkait lain. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Standar yang berlaku terkait dengan keamanan informasi

3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall*, IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5 Aspek kritis

5.1 Ketepatan dalam membuat prioritas penerapan alternatif strategi keamanan fungsional untuk mengatasi masalah keamanan dilingkungan jaringan sistem informasi organisasi yang disetujui oleh pimpinan organisasi

5.2 Ketepatan dalam membuat laporan hasil evaluasi biaya manfaat

5.3 Ketepatan dalam membuat laporan hasil analisis ekonomi

5.4 Ketepatan dalam membuat laporan hasil analisis risiko

5.5 Ketepatan dalam menyusun daftar risiko sistem informasi, analisa dampak bisnis dan rencana mitigasi

5.6 Ketepatan dalam menyusun kebijakan keamanan informasi dalam tingkatan strategis

KODE UNIT : **J.62090.006.01**

JUDUL UNIT : **Melaksanakan Kebijakan Keamanan Informasi**

DESKRIPSI : Melaksanakan kebijakan keamanan informasi sesuai dengan dokumen kebijakan keamanan informasi yang telah diotorisasi oleh pihak manajemen.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1 Mengidentifikasi aset penting dalam organisasi	1.1 Daftar aset penting dalam organisasi yang perlu dilindungi dibuat.
2 Memproteksi aset penting dalam organisasi	2.1 Daftar aset penting dalam organisasi yang rentan ancaman. 2.2 Penanganan terhadap aset penting yang rentan ancaman dibuat.
3 Melakukan pemantauan terhadap aktivitas yang rentan ancaman	3.1 Daftar aktivitas kegiatan yang perlu dijaga. 3.2 Laporan aktivitas kegiatan yang rentan ancaman dibuat.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

   2.2 Perlengkapan

   (Tidak ada.)

3. Peraturan yang diperlukan

   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam melaksanakan kebijakan keamanan informasi sesuai dengan dokumen kebijakan keamanan informasi yang telah diotorisasi oleh pihak manajemen. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Standar yang berlaku terkait dengan keamanan informasi

3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall*, IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek Kritis

5.1 Ketepatan dalam membuat penanganan aset penting yang rentan ancaman

5.2 Ketepatan dalam membuat laporan aktivitas kegiatan yang rentan ancaman

KODE UNIT : **J.62090.007.01**

JUDUL UNIT : **Mengelola Siklus Informasi (Klasifikasi, Kategorisasi, Penanggung Jawab)**

DESKRIPSI : Mengelola siklus informasi yang meliputi: klasifikasi, kategorisasi, dan penanggung-jawab yang ada di dalam organisasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi informasi sesuai klasifikasi yang meliputi: *confidential, private, sensitive, public*	1.1 Prosedur dan penanggung jawab untuk mengidentifikasi siklus informasi yang penting untuk dilindungi ditetapkan. 1.2 Kriteria dan syarat siklus informasi dibuat.
2. Menetapkan tolok ukur perlindungan informasi yang harus tetap rahasia	2.1 Prosedur dan penanggung jawab untuk mengidentifikasi informasi yang rahasia ditetapkan. 2.2 Proteksi terhadap informasi yang rahasia ditetapkan. 2.3 *Log* catatan seberapa lama informasi tetap rahasia ditetapkan.
3. Menetapkan tolok ukur siklus informasi agar konsistensi datanya tetap terjaga	3.1 Prosedur dan penanggung jawab untuk menentukan hak akses ditetapkan. 3.2 *Log file* agar dapat mengetahui siapa, kapan dan apa data yang dimodifikasi dibuat.
4. Menetapkan tolok ukur siklus informasi agar segera tersedia saat informasi diperlukan	3.1 Daftar informasi dan lamanya informasi itu perlu disimpan agar tetap ada saat diperlukan.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

2.1 Peralatan

(Tidak ada.)

2.2 Perlengkapan

(Tidak ada.)

3. Peraturan yang diperlukan

3.3 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

3.4 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam mengelola siklus informasi yang meliputi klasifikasi, kategorisasi, dan penanggung-jawab yang ada di dalam organisasi. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
    3.1 Pengetahuan
        3.1.1 Standar yang berlaku terkait dengan keamanan informasi
        3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)
        3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall*, IPS)
        3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)
    3.2 Keterampilan
        3.2.1 Mengoperasikan perangkat keras dan piranti lunak
        3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi
        3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan
    4.1 Disiplin
    4.2 Teliti
    4.3 Tanggung jawab

5. Aspek Kritis
    5.1 Ketepatan dalam menetapkan *log* catatan seberapa lama informasi tetap rahasia
    5.2 Ketepatan dalam membuat *log file* agar dapat mengetahui siapa, kapan dan apa data yang dimodifikasi

KODE UNIT : **J.62090.008.01**

JUDUL UNIT : **Melaksanakan Ketentuan Hukum yang Berlaku tentang Keamanan Informasi**

DESKRIPSI : Mematuhi dan melaksanakan hukum/regulasi keamanan sistem informasi dan segala peraturannya yang diterbitkan khusus oleh pemerintah atau badan-badan resmi terkait tentang keamanan informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mematuhi dan melaksanakan petunjuk yang terdapat pada dokumen yang diterbitkan khusus oleh pemerintah atau badan-badan resmi terkait untuk mengelola sistem operasi Lingkungan Komputasi	1.1 Dokumen yang diterbitkan khusus oleh pemerintah atau badan-badan resmi terkait untuk mengelola sistem operasi Lingkungan Komputasi diindentifikasi. 1.2 Butir-butir pokok yang terdapat pada dokumentasi tersebut dideskripsikan.
2. Menerapkan ketentuan hukum keamanan sistem dan peraturan yang sesuai dengan infrastruktur sistem teknologi informasi yang didukung	2.1 Dokumen daftar seluruh pelanggaran dan tindakannya pra solusi/*preventif*-nya atas keamanan sistem infrastruktur dan sistem Teknologi Informasi yang didukung dibuat.
3. Mematuhi hukum/regulasi keamanan sistem informasi dan segala peraturannya untuk mendukung operasi fungsional dari lingkungan jaringan	3.1 Dokumen regulasi/peraturan keamanan sistem informasi dipatuhi. 3.2 Hasil audit/rekomendasi kepatuhan pelaksanaan kegiatan sehari-hari yang terkait dengan regulasi keamanan sistem informasi yang berlaku diterapkan.
4. Mengidentifikasi dan/atau menentukan apakah sebuah insiden keamanan merupakan indikasi dari pelanggaran hukum yang memerlukan tindakan hukum tertentu	4.1 Dokumen yang terkait dengan regulasi dan /atau undang-undang tentang keamanan informasi yang berlaku diidentifikasi. 4.2 *Log* catatan insiden dan resolusinya dibuat. 4.3 Rekomendasi hasil evaluasi indikasi pelanggaran hukum diberikan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
5. Menyusun, menerapkan, dan menegakkan kebijakan dan prosedur yang mencerminkan tujuan legislatif hukum dan peraturan yang berlaku untuk lingkungan jaringan sistem informasi organisasi	5.1 Kebijakan dan prosedur legal dan peraturan yang berlaku untuk lingkungan jaringan sistem informasi organisasi disusun. 5.2 Kebijakan dan prosedur legal dan peraturan yang berlaku untuk lingkungan jaringan sistem informasi organisasi disetujui oleh pimpinan untuk diterapkan. 5.3 Hasil audit/rekomendasi pelaksanaan kebijakan dan prosedur diterapkan.
6. Memberikan dukungan dalam pengumpulan dan pelestarian bukti yang digunakan dalam proses penuntutan kejahatan komputer	6.1 Dokumen hasil kegiatan pengumpulan dan pelestarian bukti yang digunakan dalam proses penuntutan kejahatan komputer diberikan.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan
   - 2.1 Peralatan

     (Tidak ada.)
   - 2.2 Perlengkapan

     (Tidak ada.)

3. Peraturan yang diperlukan
   - 3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   - 3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam mematuhi dan melaksanakan hukum/regulasi keamanan sistem informasi dan segala peraturannya yang diterbitkan khusus oleh pemerintah atau badan-badan resmi terkait tentang keamanan informasi. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Standar yang berlaku terkait dengan keamanan informasi

3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall*, IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1. Ketepatan dalam mendeskripsikan butir-butir pokok yang terdapat pada dokumentasi tersebut

5.2. Ketepatan dalam menerapkan hasil audit/rekomendasi kepatuhan pelaksanaan kegiatan sehari-hari yang terkait dengan regulasi keamanan sistem informasi yang berlaku

5.3. Ketepatan dalam membuat *log* catatan insiden dan resolusinya

5.4. Ketepatan dalam memberikan rekomendasi hasil evaluasi indikasi pelanggaran hukum

5.5. Ketepatan dalam menerapkan kebijakan dan prosedur legal dan peraturan yang berlaku untuk lingkungan jaringan sistem informasi organisasi disetujui oleh pimpinan

5.6. Ketepatan dalam menerapkan hasil audit/rekomendasi pelaksanaan kebijakan dan prosedur

KODE UNIT : **J.62090.009.01**

JUDUL UNIT : **Mengelola Prosedur Keamanan Informasi**

DESKRIPSI : Menyusun misi, fungsi, kebijakan, dan prosedur organisasi secara aman, menerapkan petunjuk dan pedoman yang ditetapkan untuk melakukan tugas keamanan informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengintegrasikan dan menerapkan misi, fungsi, kebijakan, dan prosedur organisasi secara aman dalam lingkup strategis	1.1 Kebijakan dan prosedur keamanan informasi organisasi telah disusun. 1.2 Dokumen-dokumen yang terkait dengan misi, fungsi, kebijakan, dan prosedur organisasi diintegrasikan dengan aspek keamanan informasi. 1.3 Sosialisasi dan pelatihan tentang kebijakan keamanan informasi pada lingkup strategis telah dilaksanakan.
2. Menerapkan petunjuk dan pedoman yang ditetapkan sebelumnya untuk melakukan tugas Keamanan Informasi serta patuh terhadap beban tanggung jawab untuk setiap tugas pekerjaan	2.1 Sistem dan prosedur deteksi potensi pelanggaran keamanan telah ditetapkan.
3. Menganalisa pola dari ketidak-patuhan dan mengambil tindakan administratif yang sesuai atau tindakan terprogram untuk meminimalkan risiko pelanggaran keamanan dan ancaman dari dalam	3.1 Dokumen program tindakan dan pola dari ketidakpatuhan ditetapkan. 3.2 Dokumen hasil analisis risiko dan ancaman dari dalam dibuat. 3.3 Daftar risiko dan strategi penanganannya ditetapkan.
4. Memantau dan mengevaluasi efektifitas prosedur keamanan dari sistem strategis dan perlindungannya	4.1 Rencana kegiatan evaluasi efektifitas prosedur pengamanan pada tingkatan strategis disusun. 4.2 Laporan hasil kegiatan evaluasi efektifitas prosedur pengamanan pada tingkatan strategis dibuat.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
5. Memantau dan mengevaluasi efektifitas prosedur keamanan dari sistem strategis dan perlindungannya	5.1 Rencana kegiatan evaluasi efektifitas prosedur pengamanan pada tingkatan strategis. 5.2 Laporan hasil kegiatan evaluasi efektifitas prosedur pengamanan pada tingkatan strategis.
6. Menyiapkan, mendistribusikan, danmemelihara rencana, instruksi, pedoman, dan prosedur operasi standar tentang keamanan sistem jaringan	6.1 Dokumen rencana, instruksi, pedoman, dan prosedur operasi standar tentang keamanan sistem jaringan informasi disusun dan diperbaharui secara berkala. 6.2 Umpan balik dari pengguna akhir atas pemahaman dokumen-dokumen tersebut diatas dianalisa.
7. Melakukan pemantauan kepatuhan dan mengkaji hasil pemantauan di lingkungan jaringan sistem informasi	7.1 Rencana kegiatan pemantauan kepatuhan telah disusun. 7.2 Laporan hasil pemantauan kepatuhan dibuat.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

   2.2 Perlengkapan

   (Tidak ada.)

3. Peraturan yang diperlukan

   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian
   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam menyusun misi, fungsi, kebijakan, dan prosedur organisasi secara aman serta menerapkan petunjuk dan pedoman yang ditetapkan untuk melakukan tugas Keamanan Informasi. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:
   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.
   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.
   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
   3.1 Pengetahuan
      3.1.1 Standar yang berlaku terkait dengan keamanan informasi
      3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)
      3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall*, IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5 Aspek kritis

5.1 Ketepatan dalam melaksanakan sosialisasi dan pelatihan tentang kebijakan keamanan informasi pada lingkup strategis

5.2 Ketepatan dalam membuat laporan hasil kegiatan evaluasi efektifitas prosedur pengamanan pada tingkatan strategis

5.3 Ketepatan dalam membuat laporan hasil kegiatan evaluasi efektifitas prosedur pengamanan pada tingkatan strategis

5.4 Ketepatan dalam menganalisa umpan balik dari pengguna akhir atas pemahaman dokumen-dokumen tersebut diatas

5.5 Ketepatan dalam membuat laporan hasil pemantauan kepatuhan

KODE UNIT : **J.62090.010.01**

JUDUL UNIT : **Mengimplementasikan Prosedur Keamanan Informasi Dalam Kegiatan Pengadaan**

DESKRIPSI : Mengevaluasi, menyusun kecukupan persyaratan keamanan informasi spesifik untuk pengadaan sistem dan memonitor pelaksanaannya.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menyusun persyaratan keamanan jaringan spesifik untuk pengadaan sistem TI yang nantinya akan menjadi bagian dari dokumen pengadaan	1.1 Daftar prasyarat keamanan jaringan yang bagian dari dokumen pengadaan sistem TI organisasi disusun. 1.2 Persyaratan keamanan yang terkait dengan rencana kontinuitas operasional organisasi disetujui oleh pimpinan untuk diaplikasikan.
2. Memonitor kinerja sesuai kontrak dan secara berkala meninjau hasil evaluasi untuk kesesuaian dengan persyaratan kontrak yang berkaitan dengan keamanan lingkungan jaringan, keamanan, dan privasi	2.1 Kontrak dan persyaratan kontrak yang berkaitan dengan keamanan lingkungan jaringan, keamanan, dan privasi diidentifikasi. 2.2 Laporan kinerja kesesuaian pelaksanakan kontrak dengan persyaratannya dibuat.
3. Mengevaluasi keberadaan dan kecukupan pengamanan yang telah diusulkan atau telah dilaksanakan dalam menanggapi persyaratan yang tercantum dalam dokumen pengadaan	3.1 Rencana kegiatan evaluasi keberadaan dan kecukupan pengamanan disusun. 3.2 Laporan hasil kegiatan evaluasi keberadaan dan kecukupan pengamanan dibuat.
4. Memeriksa ketentuan keamanan terkait dari dokumen pengadaan sistem agar sesuai dengan semua kebutuhan keamanan yang telah diidentifikasi	4.1 Daftar ketentuan keamanan yang merupakan bagian dari dokumen pengadaan sistem disusun. 4.2 Laporan hasil pemeriksaan ketentuan keamanan dalam dokumen pengadaan sistem dibuat.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

   2.2 Perlengkapan

   (Tidak ada.)

3. Peraturan yang diperlukan

   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar

   4.1 Norma

   (Tidak ada.)

   4.2 Standar

   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam mengevaluasi, menyusun kecukupan persyaratan keamanan informasi spesifik untuk pengadaan sistem dan memonitor pelaksanaannya. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Standar yang berlaku terkait dengan keamanan informasi

3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam mengaplikasikan persyaratan keamanan yang terkait dengan rencana kontinuitas operasional organisasi

5.2 Ketepatan dalam mengidentifikasi kontrak dan persyaratan kontrak yang berkaitan dengan keamanan lingkungan jaringan, keamanan, dan privasi

5.3 Ketepatan dalam membuat laporan kinerja kesesuaian pelaksanakan kontrak dengan persyaratannya

5.4 Ketepatan dalam membuat laporan hasil kegiatan evaluasi keberadaan dan kecukupan pengamanan

5.5 Ketepatan dalam membuat laporan hasil pemeriksaan ketentuan keamanan dalam dokumen sistem pengadaan

KODE UNIT : **J.62090.011.01**

JUDUL UNIT : **Menerapkan Standar-Standar Keamanan Informasi yang Berlaku**

DESKRIPSI : Mengidentifikasi, menganalisis, dan memilih standar keamanan informasi yang akan dijadikan ajuan dalam menetapkan kebijakan dan prosedur keamanan informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi standar keamanan informasi (seperti SNI-ISO 27001, COBIT, dll)	1.1 Referensi standar keamanan informasi diidentifikasi. 1.2 Prioritas penerapan standar keamanan informasi organisasi disetujui oleh pimpinan organisasi.
2. Mengevaluasi komponen pokok standar keamanan untuk menentukan apakah bisa diaplikasikan secara efektif untuk kebutuhan organisasi	2.1 Daftar komponen pokok standar keamanan untuk kebutuhan organisasi disusun. 2.2 Rekomendasi hasil analisa standar keamanan untuk kebutuhan strategis organisasi dibuat.
3. Menganalisa skema akses berbasis peran/tanggung jawab/jabatan untuk implementasi keamanan informasi	3.1 Rincian pekerjaan untuk setiap peran/jabatan dalam organisasi dan akuntabilitas informasi untuk masing-masing peran/jabatan tersebut diidentifikasi. 3.2 Prosedur tentang tugas dan tanggungjawab yang terkait dengan keamanan sistem informasi dibuat.
4. Menganalisis dan memilih referensi standar keamanan dalam tingkatan strategis	4.1 Risiko sistem informasi, analisa dampak bisnis dan rencana mitigasi disusun. 4.2 Referensi untuk pembuatan kebijakan dan prosedur keamanan informasi diseleksi

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya,

harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan
   2.1 Peralatan
       (Tidak ada.)
   2.2 Perlengkapan
       (Tidak ada.)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
       (Tidak ada.)
   4.2 Standar
       4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam mengidentifikasi, menganalisis, dan memilih standar keamanan informasi yang akan dijadikan ajuan dalam menetapkan kebijakan dan prosedur keamanan informasi. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.
   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.
   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

   3.1 Pengetahuan

      3.1.1 Standar yang berlaku terkait dengan keamanan informasi

      3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

      3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

      3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

   3.2 Keterampilan

      3.2.1 Mengoperasikan perangkat keras dan piranti lunak

      3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

      3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

   4.1 Disiplin

   4.2 Teliti

   4.3 Tanggung jawab

5. Aspek kritis

   5.1 Ketepatan dalam memprioritaskan penerapan standar keamanan informasi organisasi disetujui oleh pimpinan organisasi

   5.2 Ketepatan dalam membuat rekomendasi hasil analisa standar keamanan untuk kebutuhan strategis organisasi

KODE UNIT : **J.62090.012.01**

JUDUL UNIT : **Mengaplikasikan Ketentuan/Persyaratan Keamanan Informasi**

DESKRIPSI : Menyusun persyaratan keamanan dalam prosedur operasi di lingkungan komputasi dan menerapkannya dalam kegiatan sehari-hari yang terkait dengan keamanan informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengaplikasikan persyaratan untuk program yang spesifik untuk keamanan lingkungan komputasi guna mengidentifikasi kelemahan/kerentanan	1.1 Prasyarat untuk program yang spesifik untuk keamanan lingkungan komputasi telah diterapkan. 1.2 Laporan daftar program/sistem keamanan yang telah diterapkan.
2. Menyediakan masukan tentang hal yang terkait dengan persyaratan keamanan untuk dimasukkan dalam laporan pekerjaan dan dokumen-dokumen pengadaan terkait	2.1 Daftar persyaratan keamanan yang akan dimasukan dalam dokumen pengadaan telah disusun.
3. Mengumpulkan dan memelihara data yang diperlukan untuk memenuhi persyaratan pelaporan keamanan sistem	3.1 Data yang diperlukan untuk memenuhi persyaratan pelaporan keamanan sistem dideskripsikan. 3.2 Laporan berkala keamanan sistem dibuat.
4. Mengindentifikasikan persyaratan keamanan dalam prosedur operasi di lingkungan komputasi	4.1 Dasar prasyarat keamanan yang menjadi bagian dari prosedur operasi lingkungan komputasi telah disusun. 4.2 Prosedur yang berisi prasyarat keamanan sistem informasi disetujui oleh pimpinan untuk diterapkan.
5. Menyusun persyaratan keamanan untuk perangkat keras, piranti lunak, dan penggunaan layanan yang spesifik untuk program keamanan jaringan	5.1 Daftar prasyarat keamanan untuk perangkat keras, piranti lunak, dan akuisisi layanan yang spesifik telah tersusun.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
	5.2 Persyaratan keamanan untuk perangkat keras, piranti lunak, dan akuisisi layanan yang spesifik disetujui oleh pimpinan untuk diaplikasikan.
6. Mengevaluasi dan/atau menyetujui persyaratan keamanan yang relevanterhadap kemampuan teknologi informasi yang baru.	6.1 Daftar persyaratan keamanan yang relevan terhadap kemampuan teknologi informasi yang baru dibuat. 6.2 Dokumen rekomendasi hasil analisa persyaratan keamanan yang relevan terhadap kemampuan teknologi informasi yang baru dibuat.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan
   - 2.1 Peralatan

     (Tidak ada.)
   - 2.2 Perlengkapan

     (Tidak ada.)

3. Peraturan yang diperlukan
   - 3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   - 3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam menyusun persyaratan keamanan dalam prosedur operasi di lingkungan komputasi dan menerapkannya dalam kegiatan sehari-hari yang terkait dengan keamanan informasi. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Standar yang berlaku terkait dengan keamanan informasi

3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall*, IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam menerapkan prasyarat untuk program yang spesifik untuk keamanan lingkungan komputasi

5.2 Ketepatan dalam menerapkan laporan daftar program/sistem keamanan

5.3 Ketepatan dalam membuat laporan berkala keamanan sistem

5.4 Ketepatan dalam mengaplikasikan persyaratan keamanan untuk perangkat keras, piranti lunak, dan akuisisi layanan yang spesifik disetujui oleh pimpinan.

KODE UNIT : **J.62090.013.01**

JUDUL UNIT : **Mengelola Proses Sertifikasi dan Akreditasi Untuk Keamanan Informasi**

DESKRIPSI : Menyiapkan atau melaksanakan pengawasan penyusunan sertifikasi keamanan dan dokumentasi akreditasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Memberikan saran kepada otoritas pemberi akreditasi atas setiap perubahan yang mempengaruhi postur/kondisi keamanan lingkungan jaringan sistem informasi	1.1 Kebijakan tentang keamanan sistem informasi telah disusun dan diaplikasikan. 1.2 Daftar rencana manajemen perubahan disusun. 1.3 Daftar risiko yang terkait dengan rencana manajemen perubahan telah tersusun. 1.4 Dokumen saran/rekomendasi mitigasi risiko keamanan disusun.
2. Melaksanakan penilaian risiko sistem informasi selama proses sertifikasi dan akreditasi	2.1 Referensi *best practice* untuk penerapan strategi keamanan pada tingkatan strategis diidentifikasi. 2.2 Rekomendasi hasil analisis strategi keamanan yang sesuai untuk tingkatan strategis dibuat.
3. Menyiapkan atau melaksanakan pengawasan penyusunan sertifikasi keamanan dan dokumentasi akreditasi	3.1 Rencana pengawasan penyusunan sertifikasi keamanan dan dokumentasi akreditasi disusun. 3.2 Laporan kegiatan pengawasan penyusunan sertifikasi keamanan dan dokumentasi akreditasi dibuat.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

2.1 Peralatan

(Tidak ada.)

2.2 Perlengkapan

(Tidak ada.)

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam menyiapkan atau melaksanakan pengawasan penyusunan sertifikasi Keamanan dan dokumentasi akreditasi. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Standar yang berlaku terkait dengan keamanan informasi

3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5 Aspek kritis

5.1 Ketepatan dalam menyusun rencana pengawasan penyusunan sertifikasi keamanan dan dokumentasi akreditasi

5.2 Ketepatan dalam membuat laporan kegiatan pengawasan penyusunan sertifikasi keamanan dan dokumentasi akreditasi

KODE UNIT : **J.62090.014.01**

JUDUL UNIT : **Melaksanakan Alokasi Pemisahan Tugas-tugas**

DESKRIPSI : Memisahkan tugas dan cakupan tanggung jawab untuk mengurangi kemungkinan pengubahan atan penyalahgunaan tanpa pengesahan atau tidak disengaja terhadap aset perusahaan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menerapkan prosedur untuk memastikan pengguna sistem menyadari tanggung jawab keamanan mereka sebelum memberikan akses ke sistem informasi organisasi	1.1 Prosedur tentang tanggung jawab keamanan bagi tiap pengguna telah disusun. 1.2 Hasil audit/rekomendasi pelaksanaan pemberian akses ke pengguna dilaporkan.
2. Mengatur pemisahan tugas dengan tujuan untuk mengurangi risiko	2.1 Dipastikan tidak ada seorang pun yang dapat mengubah atau menggunakan aset tanpa pengesahan dan tanpa terdeteksi. 2.2 Tugas inisiasi dan tugas pengesahan ditentukan. 2.3 Tugas yang mengurangi risiko terjadinya kolusi ditentukan. 2.4 Tugas audit dipisahkan dan fungsi lainnya.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

2.2 Perlengkapan

(Tidak ada.)

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam memisahkan tugas dan cakupan tanggung jawab untuk mengurangi kemungkinan pengubahan atan penyalahgunaan tanpa pengesahan atau tidak disengaja terhadap aset perusahaan. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Standar yang berlaku terkait dengan keamanan informasi

3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.4 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam melaporkan hasil audit/rekomendasi pelaksanaan pemberian akses ke pengguna

5.2 Ketepatan dalam menentukan tugas inisiasi dan tugas pengesahan

5.3 Ketepatan dalam menentukan tugas yang mengurangi risiko terjadinya kolusi

KODE UNIT : **J.62090.015.01**

JUDUL UNIT : **Melaksanakan Koordinasi dan Pengarahan Pelaksanaan Tugas-Tugas Keamanan Informasi**

DESKRIPSI : Melaksanakan koordinasi dan memberikan arahan kepada SDM tentang tugas-tugas keamanan informasi dan memastikan SDM tersebut memiliki kesadaran keamanan dan literasi sepadan dengan tanggung jawab yang diberikan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
5. Menunjukkan kepemimpinan dan memberikan pengarahan kepada personil-personil keamanan operasional	5.1 Daftar peraturan dan arahan yang berisi standar instruksi kepada para personil keamanan disusun.
5. Melaksanakan koordinasi dan/atau menyediakan bantuan untuk semua aplikasi posisi strategis dan operasi	5.1 Daftar layanan informasi beserta ketentuan keamanan informasi untuk tingkatan strategis disusun 5.2 Laporan kegiatan dukungan keamanan aplikasi pada tingkatan strategis dibuat.
5. Mengarahkan/memimpin tim dan/atau menyediakan dukungan untuk menyelesaikan dengan cepat atau mengurangi masalah keamanan untuk lingkungan strategis	5.1 Daftar layanan informasi beserta ketentuan keamanan informasi untuk tingkatan strategis disusun 5.2 Laporan kegiatan penanganan masalah keamanan pada tingkatan strategis dibuat.
5. Menyediakan kepemimpinan dan arahan kepada SDM jaringan sistem informasi dengan memastikan bahwa kesadaran keamanan, dasar-dasar, literasi, dan pelatihan diberikan kepada personil operasi sepadan dengan tanggung jawab mereka	5.1 Kebijakan tentang keamanan sistem informasi disusun dan diaplikasikan. 5.2 Sosialisasi dan pelatihan tentang kesadaran dan kewaspadaan keamanan sistem informasi kepada SDM terkait dilaksanakan. 5.3 Tugas dan tanggung jawab yang terkait dengan keamanan sistem informasi diaplikasikan.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan
   - 2.1 Peralatan

     (Tidak ada.)
   - 2.2 Perlengkapan

     (Tidak ada.)

3. Peraturan yang diperlukan
   - 3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   - 3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   - 4.1 Norma

     (Tidak ada.)
   - 4.2 Standar

     4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam melaksanakan koordinasi dan memberikan arahan kepada SDM tentang tugas-tugas keamanan informasi dan memastikan SDM tersebut memiliki kesadaran keamanan dan literasi sepadan dengan tanggung

jawab yang diberikan. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Standar yang berlaku terkait dengan keamanan informasi

3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam melaksanakan sosialisasi dan pelatihan tentang kesadaran dan kewaspadaan keamanan sistem informasi kepada SDM terkait

5.2 Ketepatan dalam mengaplikasikan tugas dan tanggung jawab yang terkait dengan keamanan sistem informasi

KODE UNIT : **J.62090.016.01**

JUDUL UNIT : **Mengelola SDM yang Terkait dengan Tugas-Tugas Keamanan Informasi**

DESKRIPSI : Menyusun tugas dan tanggung jawab SDM yang terkait dengan tugas-tugas keamanan informasi serta menyeleksi SDM yang tepat untuk tugas-tugas tersebut. Mengembangkan dan memelihara pengetahuan dan keterampilan yang terkait dengan keamanan informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Melakukan validasi penunjukan/penugasan pengguna untuk tugas-tugas yang terkait dengan keamanan informasi yang sensitif	1.1 Dokumen pelaksanaan tugas-tugas yang terkait dengan keamanan informasi yang sensitif kepada peran/jabatan terkait dalam organisasi dibuat. 1.2 Hasil audit/rekomendasi pelaksanaan tugas-tugas keamanan informasi oleh peran/jabatan terkait dilaporkan.
2. Merekomendasikan alokasi sumber daya yang dibutuhkan untuk secara aman mengoperasikan dan memelihara keamanan jaringan organisasi seusai dengan persyaratannya	2.1 Dokumen penugasan SDM pemeliharaan keamanan jaringan dan lingkungan komputasi diterima oleh SDM yang diberi tanggung jawab pelaksanaannya.
3. Mendapatkan dan mempertahankan sertifikasi keamanan sesuai dengan posisi/jabatan dalam organisasi	3.1 SDM yang memiliki tanggung jawab keamanan sesuai dengan peran/jabatan dalam organisasi memiliki sertifikasi keamanan yang dikeluarkan oleh badan/lembaga terkait.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

   2.2 Perlengkapan

   (Tidak ada.)

3. Peraturan yang diperlukan

   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar

   4.1 Norma

   (Tidak ada.)

   4.2 Standar

   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam menyusun tugas dan tanggung jawab SDM yang terkait dengan tugas-tugas keamanan informasi serta menyeleksi SDM yang tepat untuk tugas-tugas tersebut. Mengembangkan dan memelihara pengetahuan dan keterampilan yang terkait dengan keamanan informasi. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

   3.1 Pengetahuan

      3.1.1 Standar yang berlaku terkait dengan keamanan informasi

      3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

      3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

      3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

   3.2 Keterampilan

      3.2.1 Mengoperasikan perangkat keras dan piranti lunak

      3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

      3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

   4.1 Disiplin

   4.2 Teliti

   4.3 Tanggung jawab

5. Aspek kritis

   5.1 Ketepatan dalam membuat dokumen penugasan SDM pemeliharaan Keamanan Jaringan dan Lingkungan Komputasi diterima oleh SDM yang diberi tanggung jawab pelaksanaannya

   5.2 Ketepatan dalam menempatkan SDM yang memiliki tanggung jawab keamanan sesuai dengan peran/jabatan dalam organisasi memiliki sertifikasi keamanan yang dikeluarkan oleh badan/lembaga terkait

KODE UNIT : **J.62090.017.01**

JUDUL UNIT : **Mengelola Program Peningkatan Kepedulian dan Pelatihan Terkait dengan Keamanan Informasi**

DESKRIPSI : Melaksanakan pelatihan, pendidikan dan program untuk meningkatkan kepedulian kepada seluruh SDM organisasi terkait kebijakan dan prosedur yang sesuai dengan pekerjaannya.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Memperkenalkan kebijakan keamanan informasi dan harapan yang akan dicapai	1.1 Kebijakan keamanan informasi diterapkan. 1.2 Harapan terkait keamanan informasi diterapkan. 1.3 Kebijakan dan harapan keamanan informasi disosialisasikan
2. Menyusun materi-materi persyaratan keamanan, kewajiban legal dan pengawasan bisnis dan penggunaan fasilitas pemrosesan informasi yang benar pada setiap pelatihan	2.1 Persyaratan keamanan organisasi diidentifikasi. 2.2 Kewajiban legal organisasi dan personil organisasi diidentifikasi. 2.3 Prosedur pengawasan bisnis diidentifikasi. 2.4 Prosedur penggunaan fasilitas pemrosesan informasi yang benar dibuat.
3. Merancang pelatihan yang sesuai dengan peran, tanggung jawab dan keahlian dari setiap personil	3.1 Peran, tanggung jawab dan keahlian yang dibutuhkan pada masing-masing posisi diterapkan. 3.2 Materi-materi pelatihan yang dapat melingkupi seluruh peran, tanggung jawab dan keahlian yang dibutuhkan diidentifikasi.
4. Mengembangkan materi-materi keamanan umum, seperti ancaman-ancaman informasi, personil yang harus dihubungi untuk mendapatkan masukan tentang keamanan dan mekanisme pelaporan insiden keamanan	4.1 Informasi umum terkait keamanan informasi dibuat. 4.2 Prosedur umum terkait keamanan informasi dibuat. 4.3 Aktivitas sosialisasi dan publikasi yang efektif direncanakan dan dilaksanakan.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan
   2.1 Peralatan
   (Tidak ada.)
   2.2 Perlengkapan
   (Tidak ada.)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam melaksanakan pelatihan, pendidikan dan program untuk meningkatkan kepedulian kepada seluruh SDM organisasi terkait kebijakan dan prosedur yang sesuai dengan pekerjaannya. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Standar yang berlaku terkait dengan keamanan informasi

3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam menerapkan peran, tanggung jawab dan keahlian yang dibutuhkan pada masing-masing posisi

5.2 Ketepatan dalam mengidentifikasi materi-materi pelatihan yang dapat melingkupi seluruh peran, tanggung jawab dan keahlian yang dibutuhkan

5.3 Ketepatan dalam merencanakan dan melaksanakan aktivitas sosialisasi dan publikasi yang efektif

KODE UNIT : **J.62090.018.01**

JUDUL UNIT : **Mengelola Risiko Keamanan Informasi**

DESKRIPSI : Mengevaluasi potensi dari risiko keamanan informasi dan mengambil tindakan mitigasi yang sesuai.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengevaluasi potensi dari risiko keamanan dan mengambil tindakan koreksi dan tindakan pemulihan	1.1 Daftar risiko keamanan sistem informasi dan mitigasinya disusun. 1.2 Laporan hasil implementasi koreksi dan tindakan pemulihan dibuat.
2. Melaksanakan proses penilaian risiko	2.1 Seluruh pemilik sumber daya dan proses bisnis dilibatkan. 2.2 Kajian seluruh proses bisnis (dan tidak terbatas pada fasilitas pemrosesan informasi saja) dilaksanakan. 2.3 Hasil penilaian berupa dampak kepada keamanan informasi dianalisa. 2.4 Seluruh hasil analisa aspek risiko digabungkan, untuk mendapatkan pemahaman keseluruhan.
3. Menetapkan prosedur untuk memastikan hak akses tidak diberikan sebelum seluruh tindakan perlindungan telah diimplementasikan dan perjanjian telah ditandatangani	3.1 Risiko terkait rencana pemberian hak akses diidentifikasi. 3.2 Kesesuaian hak akses yang akan diberikan dianalisa. 3.3 Pengendalian untuk mengatasi risiko diterapkan. 3.4 Perjanjian dengan pihak yang akan diberikan hak akses dibuat.
4. Mengaudit sistem untuk mencatatkan dan mengkata*log*kan faktor-faktor yang berkaitan dengan keamanan di dalam lingkungan jaringan	4.1 Daftar risiko keamanan jaringan informasi dan mitigasinya disusun. 4.2 Rekomendasi hasil audit/rekomendasi keamanan jaringan dibuat.
5. Strategi keberlanjutan bisnis harus dikembangkan untuk menentukan pendekatan secara keseluruhan terhadap keberlanjutan bisnis	5.1 Hasil penilaian risiko digunakan sebagai input penyusunan strategi. 5.2 Strategi keberlanjutan bisnis dikomunikasikan kepada seluruh pihak yang terkait

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

   2.2 Perlengkapan

   (Tidak ada.)

3. Peraturan yang diperlukan

   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar

   4.1 Norma

   (Tidak ada.)

   4.2 Standar

   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam mengevaluasi potensi dari risiko keamanan informasi dan mengambil tindakan mitigasi yang sesuai. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Standar yang berlaku terkait dengan keamanan informasi

3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam menyusun daftar risiko keamanan sistem informasi dan mitigasinya

5.2 Ketepatan dalam membuat laporan hasil implementasi koreksi dan tindakan pemulihan

5.3 Ketepatan dalam membuat strategi keberlanjutan bisnis dikomunikasikan kepada seluruh pihak yang terkait

KODE UNIT : **J.62090.019.01**

JUDUL UNIT : **Melakukan Kajian Keamanan Informasi**

DESKRIPSI : Melakukan kajian atas tren dan pola permasalahan keamanan informasi pada sistem yang ditangani.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Meneliti, mengevaluasi, dan menyediakan umpan balik atas seluruh tren dan pola permasalahan keamanan informasi pada sistem yang ditangani	1.1 *Log* catatan insiden masalah keamanan dan solusinya dianalisa. 1.2 Daftar risiko keamanan sistem informasi dan mitigasinya dibuat. 1.3 Rekomendasi hasil evaluasi atas seluruh tren dan pola permasalahan keamanan di kebutuhan dukungan pelanggan diberikan kepada manajemen.
2. Menganalisis kajian keamanan informasi dan dokumentasinya untuk dampak strategis dan mengambil atau merekomendasikan tindakan yang tepat	2.1 Prosedur dan kebijakan kemanan informasi pada tingkatan strategis diidentifikasi. 2.2 Daftar risiko keamanan sistem informasi dan mitigasinya dianalisa. 2.3 Laporan hasil kajian keamanan informasi dan dokumentasinya untuk dampak strategis dibuat.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

   2.2 Perlengkapan

   (Tidak ada.)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian
   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam melakukan kajian atas tren dan pola permasalahan keamanan informasi pada sistem yang ditangani. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:
   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.
   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.
   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
   3.1 Pengetahuan
      3.1.1 Standar yang berlaku terkait dengan keamanan informasi
      3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.4 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam menganalisa *log* catatan insiden masalah keamanan dan solusinya.

5.2 Ketepatan dalam membuat rekomendasi hasil evaluasi atas seluruh tren dan pola permasalahan keamanan di kebutuhan dukungan pelanggan diberikan kepada manajemen.

KODE UNIT : **J.62090.020.01**

JUDUL UNIT : **Mengelola *Log***

DESKRIPSI : Menetapkan kebijakan pencatatan *log* dan melakukan kontrol berkas *log* terhadap kemungkinan diubah atau dihapus.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menetapkan kebijakan pencatatan *log* untuk menyertakan peristiwa penting	1.1 Prosedur dan kebijakan *log* dan pengarsipannya ditetapkan. 1.2 *Log* pencatatan peristiwa penting, layanan dan *proxy* dibuat. 1.3 Arsip *log* dibuat.
2. Melakukan kontrol berkas *log* terhadap kemungkinan diubah atau dihapus	2.1 Kendali akses diimplementasikan. 2.2 *Backup log* diimplementasikan.
3. Melakukan kontrol tempat menyimpan media file pencatatan terhadap kemungkinan penuh sehingga terjadi kegagalan ketika mencatat kejadian yang terjadi	3.1 Kebutuhan kapasitas media penyimpanan file pencatatan dianalisa. 3.2 Alokasi kapasitas disediakan agar mencegah terjadinya kegagalan tersebut.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

   2.2 Perlengkapan

   (Tidak ada.)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian
   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam menetapkan kebijakan pencatatan *log* dan melakukan kontrol berkas *log* terhadap kemungkinan diubah atau dihapus. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:
   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.
   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.
   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
   3.1 Pengetahuan
      3.1.1 Standar yang berlaku terkait dengan keamanan informasi
      3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.1 Teliti

4.2 Tanggung jawab

5 Aspek kritis

5.1 Ketepatan dalam menetapkan prosedur dan kebijakan *log* dan pengarsipannya.

5.2 Ketepatan dalam membuat *log* pencatatan peristiwa penting, layanan dan *proxy*.

KODE UNIT : **J.62090.021.01**

JUDUL UNIT : **Mengelola Audit Keamanan Informasi**

DESKRIPSI : Menyusun rencana dan melakukan supervisi kegiatan audit keamanan informasi meminimalkan risiko gangguan pada proses bisnis.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Melakukan kerjasama dengan pihak manajemen	1.1 Semua prosedur, kebutuhan, dan tanggung jawab didokumentasikan dengan baik. 1.2 Prosedur yang dilakukan dicatat dan dievaluasi.
2. Menetapkan kontrol yang akan diperiksa dalam ruang lingkup audit	2.1 Sumber daya dan hak akses yang dibutuhkan untuk melakukan pemeriksaan diidentifikasi. 2.2 Kebutuhan pemrosesan tambahan diidentifikasi dan dimintakan persetujuan.
3. Menetapkan peralatan untuk audit sistem informasi	3.1 Persyaratan penggunaan peralatan diidentifikasi. 3.2 Prosedur untuk menggunakan peralatan dilaksanakan sehingga penggunaan peralatan sesuai dengan persyaratan penggunaan.
4. Memisahkan peralatan audit dari sistem operasional dan pengembangan	4.1 Batasan dari sistem operasional dan sistem pengembangan diidentifikasi. 4.2 Petunjuk yang mempertegas batasan-batasan tersebut diidentifikasi.
5. Menetapkan tingkat keamanan tambahan bila dirasa perlu	5.1 Kondisi-kondisi terkait sumber informasi disebutkan. 5.2 Pihak-pihak yang terkait didalamnya diidentifikasi.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya,

harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan
   2.1 Peralatan
   (Tidak ada.)
   2.2 Perlengkapan
   (Tidak ada.)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian
   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam menyusun rencana dan melakukan supervisi kegiatan audit keamanan informasi meminimalkan risiko gangguan pada proses bisnis. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:
   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.
   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.
   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

   3.1 Pengetahuan

      3.1.1 Standar yang berlaku terkait dengan keamanan informasi

      3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

      3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

      3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

   3.2 Keterampilan

      3.2.1 Mengoperasikan perangkat keras dan piranti lunak

      3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

      3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

   4.1 Disiplin

   4.2 Teliti

   4.3 Tanggung jawab

5. Aspek kritis

   5.1 Ketepatan dalam mendokumentasikan dengan baik semua prosedur, kebutuhan, dan tanggung jawab

   5.2 Ketepatan dalam mencatat dan mengevaluasi prosedur yang dilakukan

KODE UNIT : **J.62090.022.01**

JUDUL UNIT : **Melaksanakan Evaluasi Kinerja Keamanan Informasi**

DESKRIPSI : Menganalisis kinerja sistem dan kontrol keamanan menangani potensi masalah-masalah keamanan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menganalisis kinerja sistem untuk potensi masalah-masalah keamanan	1.1 Dokumen hasil analisis kinerja sistem keamanan yang ada dibuat. 1.2 Daftar potensi ancaman keamanan yang dapat terjadi di dalam sistem disusun.
2. Menilai kinerja kontrol keamanan di dalam lingkungan jaringan	2.1 Daftar penilaian kontrol keamanan didalam lingkungan jaringan disusun.
3. Memonitor kinerja sistem dan peraturan untuk memenuhi persyaratan keamanan dan privasi dalam lingkungan komputasi	3.1 Rencana pemantauan kinerja sistem dan peraturan untuk memenuhi persyaratan keamanan dan privasi dalam lingkungan komputasi disusun. 3.2 Laporan berkala hasil pemantuan kinerja dan peraturan keamanan informasi dibuat.
4. Melacak dan melaporkan semua butir tinjauan manajemen keamanan	4.1 Rencana kegiatan pemantauan /peninjauan manajemen keamanan disusun. 4.2 Laporan hasil pemantauan/tinjauan manajemen keamanan disusun.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

2.2 Perlengkapan

(Tidak ada.)

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam menganalisis kinerja sistem dan kontrol keamanan menangani potensi masalah-masalah keamanan. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Standar yang berlaku terkait dengan keamanan informasi

3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam menyusun rencana pemantauan kinerja sistem dan peraturan untuk memenuhi persyaratan keamanan dan privasi dalam lingkungan komputasi

5.2 Ketepatan dalam membuat laporan berkala hasil pemantuan kinerja dan peraturan keamanan informasi

KODE UNIT : **J.62090.023.01**

JUDUL UNIT : **Mengelola Keamanan Fisik**

DESKRIPSI : Menggunakan batasan keamanan fisik untuk melindungi daerah yang berisikan informasi atau fasilitas pemrosesan informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menetapkan batas keamanan fisik, dengankekuatan yang disesuaikan dengan persyaratan keamanan dari aset yang dilindunginya dan hasil dari penilaian risiko	1.1 Persyaratan keamanan asset dan informasi yang dilindungi dianalisa. 1.2 Batas keamanan fisik ditetapkan. 1.3 Kekuatan batas keamanan fisik ditetapkan.
2. Menerapkan mekanisme dan prosedur pengamanan terhadap setiap pintu akses dan jendela untuk menghindari akses ilegal	2.1 Setiap pintu akses dan jendela di lokasi penyimpanan fasilitas pemrosesan informasi diidentifikasi. 2.2 Potensi pengaksesan ilegal dari pintu akses dan jendela diidentifikasi. 2.3 Risiko yang ditimbulkan dari pengaksesan ilegal dianalisa. 2.4 Prosedur pengamanan yang dapat mengatasi risiko pengaksesan ilegal, termasuk penjagaan khusus diterapkan.
3. Mengatur pemisahan secara fisik antara fasilitas pemrosesan informasi yang dikelola oleh pihak ketiga dan dikelola oleh organisasi	3.1 Fasilitas pemrosesan informasi yang dikelola oleh pihak ketiga dan organisasi diidentifikasi. 3.2 Penempatan fasilitas pemrosesan informasi yang dikelola oleh pihak ketiga dan internal organisasi diatur.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya,

harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan
   2.1 Peralatan
       (Tidak ada.)
   2.2 Perlengkapan
       (Tidak ada.)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
       (Tidak ada.)
   4.2 Standar
       4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam menggunakan batasan keamanan fisik untuk melindungi daerah yang berisikan informasi atau fasilitas pemrosesan informasi. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:
   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.
   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.
   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

   3.1 Pengetahuan

      3.1.1 Standar yang berlaku terkait dengan keamanan informasi

      3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

      3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

      3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

   3.2 Keterampilan

      3.2.1 Mengoperasikan perangkat keras dan piranti lunak

      3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

      3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

   4.1 Disiplin

   4.2 Teliti

   4.3 Tanggung jawab

5. Aspek kritis

   5.1 Ketepatan dalam menerapkan prosedur pengamanan yang dapat mengatasi risiko pengaksesan ilegal, termasuk penjagaan khusus

   5.2 Ketepatan dalam mengatur penempatan fasilitas pemrosesan informasi yang dikelola oleh pihak ketiga dan internal organisasi

KODE UNIT : **J.62090.024.01**

JUDUL UNIT : **Melaksanakan Pencatatan *Asset***

DESKRIPSI : Mencatat dan mengkatalogkan seluruh aset yaitu perangkat keras, piranti lunak, data, dan fasilitas-fasilitas lainnya.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mencatat dan mengkatalogkan seluruh aset ke dalam sistem manajemen kelemahan/kerentanan	1.1 Dokumentasi pencatatan yang terperinci atas seluruh asset yang masuk kedalam manajemen sistem kerentanan dibuat.
2. Memastikan bahwa seluruh perangkat keras, piranti lunak, data, dan fasilitas-fasilitas lainnya telah diarsipkan, disanitasikan, atau dibuang sesuai dengan tata cara yang konsisten dengan rencana keamanan dan kebutuhan kemanan	2.1 Rencana pengarsipan/ penghapusan perangkat keras, piranti lunak, data, dan fasilitas-fasilitas lainnya yang disesuaikan dengan kebijakan dan prosedur keamanan yang berlaku disusun. 2.2 Laporan hasil kegiatan pengarsipan dan/atau penghapusan perangkat keras, piranti lunak, data, dan fasilitas-fasilitas lainnya dibuat.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

   2.2 Perlengkapan

   (Tidak ada.)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian
   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam mencatat dan mengkata*log*-kan seluruh aset yaitu perangkat keras, piranti lunak, data, dan fasilitas-fasilitas lainnya. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:
   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.
   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.
   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
   3.1 Pengetahuan
      3.1.1 Standar yang berlaku terkait dengan keamanan informasi
      3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam menyusun rencana pengarsipan/penghapusan perangkat keras, piranti lunak, data, dan fasilitas-fasilitas lainnya yang disesuaikan dengan kebijakan dan prosedur keamanan yang berlaku

5.2 Ketepatan dalam membuat laporan hasil kegiatan pengarsipan dan/atau penghapusan perangkat keras, piranti lunak, data, dan fasilitas-fasilitas lainnya

KODE UNIT : **J.62090.025.01**

JUDUL UNIT : **Mengelola Sistem Pertahanan dan Perlindungan Keamanan Informasi**

DESKRIPSI : Mengidentifikasi, menyusun dan mengimplementasikan kebijakan sistem pertahanan untuk perlindungan informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menetapkan metodologi dan proses untuk aktivitas keamanan informasi	1.1 Metode analisa risiko diidentifikasi dan ditetapkan. 1.2 Proses pengelolaan risiko ditetapkan. 1.3 Klasifikasi informasi ditetapkan.
2. Mengkoordinasikan aktivitas terkait keamanan informasi dengan seluruh perwakilan dari setiap bagian dari organisasi yang memiliki peran dan fungsi kerja yang relevan	2.1 Kesesuaian aktivitas keamanan dengan kebijakan keamanan informasi dipantau. 2.2 Cara untuk menangani ketidaksesuaian dengan kebijakan, teridentifikasi.
3. Melindungi peralatan akibat kerusakan fisik oleh personil	3.1 Peraturan untuk meminimalkan risiko ancaman fisik, seperti pencurian, kebakaran, ledakan, asap, air, debu, getaran, efek kimia, interferensi elektris, interferensi komunikasi, radiasi elektromagnetik dan vandalisme diterapkan.
4. Melaksanakan dan memantau perlindungan keamanan untuk sistem infrastruktur dan penggunaan teknologi informasi sesuai dengan rencana implementasi dan prosedur operasi standar	4.1 Laporan pelaksanaan hasil pemantauan perlindungan keamanan sistem infrastruktur dibuat. 4.2 *Log* audit hasil pemantauan perlindungan keamanan atas prosedur operasi standar dibuat.
5. Menetapkan pendekatan manajemen terhadap penggunaan kontrol kriptografi pada perusahaan	5.1 Tingkat proteksi informasi diidentifikasi, termasuk tipe, kekuatan dan kualitas algoritma enscriptsi yang digunakan. 5.2 Standar yang akan digunakan ditentukan, dengan mempertimbangkan efektivitas implementasinya di organisasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
	5.3 Batasan regulasi yang mengatur penggunaan teknik kriptografi diidentifikasi. 5.4 Penggunaan kriptografi untuk keperluan integritas dan autentifikasi dianalisa.
6. Menetapkan pendekatan pengelolaan kunci kriptografi	6.1 Metode perlindungan kunci kriptografi ditetapkan. 6.2 Mekanisme mendapatkan kembali kunci kriptografi karena kehilangan atau kerusakan ditetapkan. 6.3 Penggunaan enkripsi bagi perlindungan terkait pengiriman informasi sensitif dengan media *mobile* atau *removeable*, atau melalui kabel komunikasi ditetapkan.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan
   - 2.1 Peralatan

     (Tidak ada.)
   - 2.2 Perlengkapan

     (Tidak ada.)

3. Peraturan yang diperlukan
   - 3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   - 3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam mengidentifikasi, menyusun dan mengimplementasikan kebijakan sistem pertahanan untuk perlindungan informasi. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Standar yang berlaku terkait dengan keamanan informasi

3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkanDisiplin

4.1 Teliti

4.2 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam memantau kesesuaian aktivitas keamanan dengan kebijakan keamanan informasi

5.2 Ketepatan dalam mengidentifikasi cara untuk menangani ketidaksesuaian dengan kebijakan

KODE UNIT : **J.62090.026.01**

JUDUL UNIT : **Menyediakan Dukungan Keamanan Bagi Pengguna**

DESKRIPSI : Menyediakan dukungan keamanan bagi para pengguna akhir untuk semua sistem operasi, infrastruktur teknologi informasi, perangkat, dan aplikasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menyediakan dukungan keamanan bagi para pengguna akhir untuk semua sistem operasi, infrastruktur teknologi informasi, perangkat, dan aplikasi	1.1 Kebijakan, prasyarat dan Prosedur keamanan yang terkait diaplikasikan dalam konfigurasi sistem operasi, insfrastruktur teknologi informasi, perangkat dan aplikasi diidentifikasi. 1.2 Laporan kegiatan dukungan keamanan bagi pengguna akhir dibuat. 1.3 Laporan berkala konfigurasi sistem keamanan dibuat.
2. Melaksanakan dukungan keamanan untuk para pelanggan termasuk instalasi, konfigurasi, pembetulan masalah, pemberian bantuan untuk pelanggan, dan juga memberikan pelatihan, sebagai tanggapan dari kebutuhan pelanggan atas sistem teknologi jaringan	2.1 Daftar komponen-komponen yang sudah terinstalasi dan terkonfigurasi beserta kelengkapan administratif dukungan lainnya disusun.
3. Menyediakan dukungan bagi para pengguna akhir untuk semua aplikasi yang terkait untuk keamanan sistem jaringan	3.1 Daftar dukungan yang diberikan kepada pengguna akhir yang berkaitan dengan keamanan jaringan disusun.
4. Memberikan dukungan untuk keamanan pelayanan pengguna sesuai dengan persyaratan performa yang ada.	4.1 Daftar/kata*log* layanan sistem informasi disusun. 4.2 Prosedur dan kebijakan, dan standar keamanan informasi untuk pengguna diterapkan. 4.3 Laporan berkala kegiatan dukungan untuk keamanan pelayanan pengguna dibuat.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
5. Memberikan dukungan untuk pengembangan kebijakan, prosedur, dan standar untuk keamanan pelayanan pengguna.	5.1 Daftar/cata*log* layanan sistem informasi disusun. 5.2 Prosedur dan kebijakan, dan standar keamanan informasi untuk pengguna diidentifikasi.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan
   - 2.1 Peralatan

     (Tidak ada.)
   - 2.2 Perlengkapan

     (Tidak ada.)

3. Peraturan yang diperlukan
   - 3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   - 3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   - 4.1 Norma

     (Tidak ada.)
   - 4.2 Standar

     4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam menyediakan dukungan keamanan bagi para pengguna akhir untuk semua sistem operasi, infrastruktur teknologi informasi, perangkat, dan aplikasi. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

   3.1 Pengetahuan

   3.1.1 Standar yang berlaku terkait dengan keamanan informasi

   3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

   3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall*, IPS)

   3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

   3.2 Keterampilan

   3.2.1 Mengoperasikan perangkat keras dan piranti lunak

   3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

   3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan
    4.1 Disiplin
    4.2 Teliti
    4.3 Tanggung jawab

5. Aspek kritis
    5.1 Ketepatan dalam membuat laporan berkala kegiatan dukungan untuk keamanan pelayanan pengguna
    5.2 Ketepatan dalam mengidentifikasi prosedur dan kebijakan, dan standar keamanan informasi untuk pengguna

KODE UNIT : **J.62090.027.01**

JUDUL UNIT : **Mengimplementasikan Konfigurasi Keamanan Informasi**

DESKRIPSI : Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi untuk menjamin bahwa peralatan yang dikelola patuh dan sesuai dengan kebijakan keamanan, prosedur keamanan, dan juga kebutuhan teknis yang ada.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi	1.1 Laporan berkala sistem konfigurasi keamanan dibuat. 1.2 *Log* deteksi pelanggaran keamanan dibuat.
2. Mengkonfigurasi, mengoptimalkan, dan menguji server jaringan, *hub*, *router*, dan *switch* untuk menjamin bahwa peralatan tersebut patuh dan sesuai dengan kebijakan keamanan, prosedur keamanan, dan juga kebutuhan teknis yang ada	1.1 Daftar konfigurasi, dan optimasi yang telah dilakukan kepada semua peralatan seperti *hub*, *router*, dan lainnya disusun. 1.2 Laporan kepatutan dan kepatuhan atas kebijakan dan prosedur keamanan terhadap konfigurasi untuk semua peralatan seperti *hub*, *router*, dan lainnya dibuat.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

2.2 Perlengkapan

(Tidak ada.)

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi untuk menjamin bahwa peralatan yang dikelola patuh dan sesuai dengan kebijakan keamanan, prosedur keamanan, dan juga kebutuhan teknis yang ada. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
    3.1 Pengetahuan
        3.1.1 Standar yang berlaku terkait dengan keamanan informasi
        3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)
        3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)
        3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)
    3.2 Keterampilan
        3.2.1 Mengoperasikan perangkat keras dan piranti lunak
        3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi
        3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan
    4.1 Disiplin
    4.2 Teliti
    4.3 Tanggung jawab

5. Aspek kritis
    5.1 Ketepatan dalam membuat laporan berkala sistem konfigurasi keamanan
    5.2 Ketepatan dalam membuat *log* deteksi pelanggaran keamanan dibuat
    5.3 Ketepatan dalam membuat laporan kepatutan dan kepatuhan atas kebijakan dan prosedur keamanan terhadap konfigurasi untuk semua peralatan seperti *hub*, *router*, dan lainnya

KODE UNIT : **J.62090.028.01**

JUDUL UNIT : **Mengelola *Script* Keamanan Informasi**

DESKRIPSI : Menulis dan meremajakan *script* yang dibutuhkan untuk menjamin keamanan informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menulis dan merawat *script* terkait keamanan informasi untuk lingkungan jaringan	1.1 Dokumentasi *script* untuk lingkungan jaringan dibuat. 1.2 Kemampuan menulis *script* untuk lingkungan jaringan didemonstrasikan.
2. Menulis dan meremajakan *script* yang dibutuhkan untuk menjamin keamanan lingkungan strategis	2.1 Dokumentasi *script* untuk keamanan informasi ditingkat strategis dibuat. 2.2 Kemampuan menulis *script* untuk lingkungan strategis didemonstrasikan.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan
   - 2.1 Peralatan

     (Tidak ada.)
   - 2.2 Perlengkapan

     (Tidak ada.)

3. Peraturan yang diperlukan
   - 3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian
   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam menulis dan meremajakan *script* yang dibutuhkan untuk menjamin keamanan informasi. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:
   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.
   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.
   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
   3.1 Pengetahuan
      3.1.1 Standar yang berlaku terkait dengan keamanan informasi
      3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)
      3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam membuat dokumentasi *script* untuk lingkungan jaringan

5.2 Ketepatan dalam membuat dokumentasi *script* untuk keamanan informasi ditingkat strategis

KODE UNIT : **J.62090.029.01**

JUDUL UNIT : **Mengelola *Perimeter* Keamanan**

DESKRIPSI : Melaksanakan instalasi dan konfigurasi sistem pertahanan *perimeter*.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Melaksanakan instalasi dan konfigurasi sistem pertahanan *perimeter* (termasuk sistem deteksi intrusi, *firewall*, sensor *grid*, dll)	1.1 Analisa kebutuhan komponen system pertahanan *perimeter* dilaksanakan. 1.2 Daftar komponen sistem pertahanan *perimeter* disusun. 1.3 Sistem pertahanan *perimeter* dipasang dan diatur konfigurasinya.
2. Memelihara sistem pertahanan *perimeter*	2.1 Catatan pemeliharaan sistem pertahanan *perimeter* dibuat. 2.2 *Log* insiden dan responnya yang terkait dengan sistem pertahanan *perimeter* dibuat.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

   2.2 Perlengkapan

   (Tidak ada.)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian
   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam melaksanakan instalasi dan konfigurasi sistem pertahanan *perimeter*. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:
   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.
   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.
   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
   3.1 Pengetahuan
      3.1.1 Standar yang berlaku terkait dengan keamanan informasi
      3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam memasang dan mengatur konfigurasi sistem pertahanan *perimeter*

5.2 Ketepatan dalam membuat catatan pemeliharaan sistem pertahanan *perimeter*

5.3 Ketepatan dalam membuat *log* insiden dan responnya yang terkait dengan sistem pertahanan *perimeter*

KODE UNIT : **J.62090.030.01**

JUDUL UNIT : **Melakukan Instalasi Piranti Lunak**

DESKRIPSI : Melaksanakan instalasi, pengujian, pemeliharaan, dan peremajaan piranti lunak dan perangkat keras sistem informasi sesuai persyaratan keamanan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Melakukan instalasi dan mengoperasikan sistem Teknologi Informasi dengan tata cara pengujian yang sama sekali tidak mengubah struktur kode pemrograman dan melanggar standar pengamanan	1.1 Dokumen petunjuk pelaksanaan bagi kegiatan instalasi yang sudah di otorisasi sebelumnya diterapkan. 1.2 Kebijakan, prasyarat instalasi dan pengoperasian sistem Teknologi Informasi yang telah disepakati bersama disusun.
2. Melaksanakan instalasi, pengujian, pemeliharaan, dan peremajaan piranti lunak dan perangkat keras sistem operasi sistem teknologi informasi untuk memenuhi persyaratan keamanan	2.1 Daftar komponen yang sudah diinstalasi, diuji, dan diremajakan disusun. 2.2 Dokumentasi pengujian hasil instalasi dan relevansi terhadap uji coba persyaratan keamanan dibuat.
3. Melaksanakan instalasi, pengujian,perawatan, dan peremajaan piranti lunak dankeras sistem operasi jaringan agar sesuai dengan kebutuhan atas keamanan	3.1 Dokumen petunjuk pelaksanaan ketentuan keamanan bagi kegiatan instalasi, pengujian, perawatan, dan peremajaan piranti lunak dan keras sistem operasi jaringan dibuat. 3.2 Laporan hasil kegiatan instalasi, pengujian, perawatan, dan peremajaan piranti lunak dan keras sistem operasi jaringan dibuat.
4. Mendukung instalasi perangkat keras baru maupun perubahan, sistem operasi, dan aplikasi piranti lunak memastikan integrasi dengan persyaratan keamanan untuk tingkatan strategis	4.1 Kebijakan dan prosedur ketentuan keamanan bagi kegiatan instalasi perangkat keras baru maupun perubahan, sistem operasi, dan aplikasi piranti lunak di tingkatan strategis diaplikasikan. 4.2 Laporan hasil kegiatan instalasi perangkat keras baru maupun perubahan, sistem operasi, dan aplikasi piranti lunak di tingkatan strategis dibuat.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

   2.2 Perlengkapan

   (Tidak ada.)

3. Peraturan yang diperlukan

   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar

   4.1 Norma

   (Tidak ada.)

   4.2 Standar

   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam melaksanakan instalasi, pengujian, pemeliharaan, dan peremajaan piranti lunak dan perangkat keras sistem informasi sesuai persyaratan keamanan. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Standar yang berlaku terkait dengan keamanan informasi

3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis
    5.1 Ketepatan dalam menyusun kebijakan, prasyarat instalasi dan pengoperasian sistem teknologi informasi yang telah disepakati bersama
    5.2 Ketepatan dalam membuat dokumentasi pengujian hasil instalasi dan relevansi terhadap uji coba persyaratan keamanan
    5.3 Ketepatan dalam membuat laporan hasil kegiatan instalasi, pengujian, perawatan, dan peremajaan piranti lunak dan keras sistem operasi jaringan
    5.4 Ketepatan dalam membuat laporan hasil kegiatan instalasi perangkat keras baru maupun perubahan, sistem operasi, dan aplikasi piranti lunak di tingkatan strategis

KODE UNIT : **J.62090.031.01**

JUDUL UNIT : **Mengelola Aspek Keamanan Sistem Informasi pada Setiap Kegiatan *Upgrade*/Peremajaan Sistem Informasi**

DESKRIPSI : Mengelola implikasi teknologi baru atau teknologi yang diremajakan terhadap program keamanan teknologi informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi implikasi teknologi baru atau teknologi yang diremajakan (*upgrade*) terhadap program keamanan teknologi informasi	1.1 Daftar teknologi baru atau teknologi yang diremajakan (*upgrade*) disusun. 1.2 Laporan hasil analisa implikasi teknologi baru atau teknologi yang diremajakan (*upgrade*) terhadap program keamanan teknologi informasi dibuat.
2. Menafsirkan dan atau menyetujui persyaratan keamanan yang relevan terhadap kemampuan teknologi informasi yang baru	2.1 Daftar persyaratan keamanan yang relevan terhadap kemampuan teknologi informasi yang baru disusun. 2.2 Dokumen rekomendasi hasil analis persyaratan keamanan yang relevan terhadap kemampuan teknologi informasi baru dibuat.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

   2.2 Perlengkapan

   (Tidak ada.)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian
   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam mengelola implikasi teknologi baru atau teknologi yang diremajakan terhadap program keamanan Teknologi Informasi. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:
   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.
   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.
   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
   3.1 Pengetahuan
      3.1.1 Standar yang berlaku terkait dengan keamanan informasi
      3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan

Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam membuat laporan hasil analisa implikasi teknologi baru atau teknologi yang diremajakan (*upgrade*) terhadap program keamanan teknologi informasi

5.2 Ketepatan dalam menyusun daftar persyaratan keamanan yang relevan terhadap kemampuan teknologi informasi yang baru

5.3 Ketepatan dalam membuat dokumen rekomendasi hasil analis persyaratan keamanan yang relevan terhadap kemampuan teknologi informasi baru

KODE UNIT : **J.62090.032.01**

JUDUL UNIT : **Menerapkan Kontrol Akses Berdasarkan Konsep/Metodologi yang telah Ditetapkan**

DESKRIPSI : Menerapkan kontrol akses Lingkungan Komputasi yang sesuai serta melakukan kontrol dan pengawasan pada setiap pengguna yang memiliki akses khusus menjalankan fungsi keamanan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menerapkan kontrol akses lingkungan komputasi yang sesuai	1.1 Sistem dan prosedur kontrol akses yang ditetapkan dideskripsikan. 1.2 *Log* untuk setiap kegiatan akses secara rinci dibuat.
2. Melaksanakan kebijakan organisasi dan kebijakan *password* organisasi	2.1 Dokumen kebijakan *password* dan penggunaannya ditetapkan. 2.2 Laporan atas penerapan sistem *password* yang ada dibuat.
3. Mengelola akun hak jaringan dan hak akses ke sistem jaringan dan infrastrukturnya	3.1 Daftar akun beserta hak akses ke dalam sistem dibuat. 3.2 Daftar hak-hak penting yang diberikan kepada pengguna tertentu didefinisikan.
4. Mengimplementasikan peringatan secara *online* untuk menginformasikan para pengguna atas peraturan akses dari seluruh infrastruktur dan penggunaan sistem teknologi informasi	4.1 Sistem *online* dari daftar peringatan yang telah terjadi selama akses penggunaan infrastruktur dan sistem teknologi informasi tersebut dibuat. 4.2 Laporan pelaksanaan peringatan secara *online* dibuat. 4.3 Catatan *log* dari daftar peringatan yang sudah terjadi dan kondisi terakhir masingmasing peringatan tersebut dibuat.
5. Menyusun prosedur untuk memastikan pengguna sistem menyadari tanggung jawab keamanan mereka sebelum memberikan akses ke sistem informasi organisasi	5.1 Prosedur tentang tanggung jawab keamanan bagi tiap pengguna disusun. 5.2 Hasil audit/rekomendasi pelaksanaan pemberian akses ke pengguna diterapkan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
6. Melakukan kontrol dan pengawasan pada setiap pengguna yang memiliki akses khusus menjalankan fungsi keamanan agar menerima pelatihan keamanan dasar dan berkelanjutan serta mendapatkan sertifikasi yang sesuai untuk melaksanakan tugas keamanan	6.1 Pelatihan keamanan dasar dan berkelanjutan dilaksanakan untuk SDM yang memiliki akses khusus menjalankan fungsi keamanan. 6.2 Sertifikasi keamanan yang dikeluarkan oleh badan/lembaga terkait dimiliki oleh SDM yang memiliki akses khusus menjalankan fungsi keamanan.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan
   - 2.1 Peralatan

     (Tidak ada.)
   - 2.2 Perlengkapan

     (Tidak ada.)

3. Peraturan yang diperlukan
   - 3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   - 3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   - 4.1 Norma

     (Tidak ada.)

4.2 Standar

4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam menerapkan kontrol akses Lingkungan Komputasi yang sesuai serta melakukan kontrol dan pengawasan pada setiap pengguna yang memiliki akses khusus menjalankan fungsi keamanan. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

   4.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

   4.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

   4.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

   3.1 Pengetahuan

   3.1.1 Standar yang berlaku terkait dengan keamanan informasi

   3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

   3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

   3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam mendeskripsikan sistem dan prosedur kontrol akses yang ditetapkan

5.2 Ketepatan dalam membuat *log* untuk setiap kegiatan akses secara rinci

5.3 Ketepatan dalam membuat laporan atas penerapan sistem *password* yang ada

5.4 Ketepatan dalam membuat laporan pelaksanaan peringatan secara *online*

5.5 Ketepatan dalam membuat catatan *log* dari daftar peringatan yang sudah terjadi dan kondisi terakhir masing-masing peringatan tersebut

KODE UNIT : **J.62090.033.01**

JUDUL UNIT : **Mengidentifikasi Serangan-Serangan Terhadap Kontrol Akses**

DESKRIPSI : Mengidentifikasi serangan-serangan terhadap kontrol akses lingkungan komputasi yang sesuai serta melakukan kontrol dan pengawasan pada setiap pengguna yang memiliki akses khusus menjalankan fungsi keamanan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mendeteksi potensi serangan-serangan yang dapat dilakukan terhadap kontrol akses, mengambil tindakan yang sesuai untuk melaporkan kejadian tersebut sesuai dengan peraturan dan mengurangi dampak yang merugikan	1.1 Laporan deteksi potensi serangan-serangan yang dapat dilakukan terhadap kontrol akses beserta tindakan pengamanan yang telah dilaksanakan dibuat.
2. Memeriksa seluruh potensi serangan-serangan yang dapat dilakukan terhadap kontrol akses untuk menentukan apakah kebijakan lingkungan teknologi jaringan telah dilanggar, menganalisa dan mencatat seluruh dampak dan juga menjaga barang bukti	2.1. Daftar seluruh pelanggaran, hasil analisa, dan pencatatan dampak negatif yang terjadi dari adanya pelanggaran kebijakan disusun. 2.2. Jumlah potensi serangan-serangan yang dapat dilakukan terhadap kontrol akses yang ada di dalam suatu sistem Teknologi Informasi diidentifikasi.
3. Mengidentifikasi kerentanan serangan-serangan yang dapat dilakukan terhadap kontrol akses yang dari rencana implementasi atau kerentanan yang tidak terdeteksi pada saat uji coba	3.1 Daftar potensi serangan-serangan yang dapat dilakukan terhadap kontrol akses yang sudah terdeteksi dalam fase uji coba maupun yang tidak terdeteksi dalam fase uji coba disusun. 3.2 Daftar kerentanan serangan-serangan yang dapat terjadi terhadap kontrol akses dan solusinya masing-masing disusun.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
4. Melakukan tinjauan perlindungan keamanan tertentu akibat serangan-serangan yang dapat dilakukan terhadap kontrol akses untuk menentukan masalah keamanan (yang diidentifikasi dalam rencana yang telah disetujui) telah sepenuhnya ditangani	2.1 Laporan hasil kegiatan tinjauan perlindungan keamanan akibat serangan-serangan yang dapat dilakukan terhadap kontrol akses dibuat.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan
   2.1 Peralatan

   (Tidak ada.)

   2.2 Perlengkapan

   (Tidak ada.)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   4.1 Norma

   (Tidak ada.)

4.2 Standar

4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam mengidentifikasi serangan-serangan terhadap kontrol akses Lingkungan Komputasi yang sesuai serta melakukan kontrol dan pengawasan pada setiap pengguna yang memiliki akses khusus menjalankan fungsi keamanan. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

   3.1 Pengetahuan

   3.1.1 Standar yang berlaku terkait dengan keamanan informasi

   3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

   3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

   3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam membuat laporan deteksi potensi serangan-serangan yang dapat dilakukan terhadap kontrol akses beserta tindakan pengamanan yang telah dilaksanakan

5.2 Ketepatan dalam mengidentifikasi potensi serangan-serangan yang dapat dilakukan terhadap kontrol akses yang ada di dalam suatu sistem teknologi informasi

5.3 Ketepatan dalam menyusun daftar kerentanan serangan-serangan yang dapat terjadi terhadap kontrol akses dan solusinya masing-masing

5.4 Ketepatan dalam membuat laporan hasil kegiatan tinjauan perlindungan keamanan akibat serangan-serangan yang dapat dilakukan terhadap kontrol akses

KODE UNIT : **J.62090.034.01**

JUDUL UNIT : **Mengkaji Efektivitas Penerapan Kontrol Akses**

DESKRIPSI : Melakukan pengkajian efektivitas penerapan kontrol akses lingkungan komputasi yang sesuai pada setiap pengguna yang memiliki akses khusus menjalankan fungsi keamanan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengevaluasi kontrol akses yang pernah ditetapkan	1.1 Sistem dan prosedur kontrol akses yang mengkaji efektivitas penerapan kontrol akses ditetapkan. 1.2 *Log* untuk setiap kegiatan kontrol akses secara rinci per periode di evaluasi. 1.3 Daftar perubahan kontrol akses hasil evaluasi dibuat.
2. Mengevaluasi kebijakan organisasi dan kebijakan *password* organisasi yang pernah ditetapkan	2.1 Dokumen kebijakan *password* dan penggunaannya dievaluasi dan diubah sesuai kondisi terkini. 2.2 Laporan atas penerapan sistem *password* yang ada dievaluasi.
3. Mengevaluasi pengelolaan akun hak jaringan dan hak akses ke sistem jaringan dan infrastrukturnya	3.1 Daftar akun beserta hak akses ke dalam system dievaluasi. 3.2 Daftar hak-hak penting yang diberikan kepada pengguna tertentu dievaluasi dan disesuaikan dengan kondisi terkini.
4. Mengevaluasi pengimplementasian peringatan secara *online* untuk menginformasikan para pengguna atas peraturan akses dari seluruh infrastruktur dan penggunaan sistem teknologi informasi	4.1 Sistem *online* dari daftar peringatan yang telah terjadi selama akses penggunaan infrastruktur dan sistem teknologi informasi tersebut dievaluasi dan disesuaikan dengan kondisi terkini. 4.2 Laporan pelaksanaan peringatan secara *online* dievaluasi dan disesuaikan dengan kondisi terkini. 4.3 Catatan *log* dari daftar peringatan yang sudah terjadi dan kondisi terakhir masingmasing peringatan tersebut dievaluasi dan disesuaikan dengan kondisi terkini.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
5. Mengevaluasi prosedur untuk memastikan pengguna sistem menyadari tanggung jawab keamanan mereka sebelum memberikan akses ke sistem informasi organisasi	5.1 Prosedur tentang tanggung jawab keamanan bagi tiap pengguna dievaluasi dan disesuaikan dengan kondisi terkini. 5.2 Hasil audit/rekomendasi pelaksanaan pemberian akses ke pengguna dievaluasi dan disesuaikan dengan kondisi terkini.
6. Mengevaluasi kontrol dan pengawasan pada setiap pengguna yang memiliki akses khusus menjalankan fungsi keamanan agar menerima pelatihan keamanan dasar dan berkelanjutan serta mendapatkan sertifikasi yang sesuai untuk melaksanakan tugas keamanan	6.1 Pelaksanaan pelatihan keamanan dasar dan berkelanjutan untuk SDM yang memiliki akses khusus menjalankan fungsi keamanan dievaluasi dan diselenggarakan dengan kondisi terkini. 6.2 Pembaharuan/peremajaan sertifikasi keamanan yang dikeluarkan oleh badan/lembaga terkait dimiliki oleh SDM yang memiliki akses khusus menjalankan fungsi keamanan bagi yang sudah memiliki.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

   2.2 Perlengkapan

   (Tidak ada.)

3. Peraturan yang diperlukan

   3.3 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

3.4 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian
   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam melakukan pengkajian efektivitas penerapan kontrol akses Lingkungan Komputasi yang sesuai pada setiap pengguna yang memiliki akses khusus menjalankan fungsi keamanan. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:
   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.
   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.
   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
   3.1 Pengetahuan
      3.1.1 Standar yang berlaku terkait dengan keamanan informasi
      3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam mengevaluasi dan menyesuaikan sistem dan prosedur kontrol akses yang pernah ditetapkan dengan kondisi terkini

5.2 Ketepatan dalam mengevaluasi dan menyesuaikan *log* untuk setiap kegiatan akses secara rinci dengan kondisi terkini

5.3 Ketepatan dalam mengevaluasi dan menyesuaikan laporan atas penerapan sistem *password* yang ada dengan kondisi terkini

5.4 Ketepatan dalam mengevaluasi dan menyesuaikan laporan pelaksanaan peringatan secara *online* dengan kondisi terkini

5.5 Ketepatan dalam mengevaluasi dan menyesuaikan catatan *log* dari daftar peringatan yang sudah terjadi dan kondisi terakhir masing-masing peringatan tersebut dengan kondisi terkini

KODE UNIT : **J.62090.035.01**

JUDUL UNIT : **Mengelola Siklus Pemberian Akses**

DESKRIPSI : Mengelola siklus pemberian akses Lingkungan Komputasi yang sesuai pada setiap pengguna yang memiliki akses khusus menjalankan fungsi keamanan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mematuhi prosedur dan tata cara pengelolaan siklus pemberian akses	1.1 Dokumen kebijakan pengelolaan siklus pemberian akses ditetapkan. 1.2 Laporan kepatutan dan kepatuhan atas pengubahan siklus pemberian akses ke sistem jaringan dan infrastrukturnya dibuat. 1.3 *Log* catatan hasil pengubahan siklus pemberian akses ke sistem jaringan dan infrastrukturnya dibuat.
2. Mengawasi atau mengelola pengelolaan siklus pemberian akses	2.1 Daftar akun beserta hak akses ke dalam sistem jaringan dan infrastrukturnya yang mendapat siklus pemberian akses dibuat. 2.2 Daftar hak-hak penting yang diberikan kepada pengguna tertentu yang mendapat siklus pemberian akses didefinisikan. 2.3 Laporan hasil pengerjaan siklus pemberian akses dibuat.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

2.2 Perlengkapan

(Tidak ada.)

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam mengelola siklus pemberian akses lingkungan komputasi yang sesuai pada setiap pengguna yang memiliki akses khusus menjalankan fungsi keamanan. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Standar yang berlaku terkait dengan keamanan informasi

3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam membuat *log* catatan hasil pengubahan siklus pemberian akses ke sistem jaringan dan infrastrukturnya

5.2 Ketepatan dalam membuat laporan pengerjaan siklus pemberian akses

KODE UNIT : **J.62090.036.01**

JUDUL UNIT : **Melaksanakan Uji Coba Sistem Pertahanan Keamanan Informasi**

DESKRIPSI : Melaksanakan uji coba konfigurasi pengamanan yang telah disesuaikan dengan rencana uji coba dan prosedur-prosedurnya.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Melaksanakan uji coba konfigurasi pengamanan yang telah disesuaikan dengan rencana uji coba dan prosedur-prosedurnya	1.1 Dokumen hasil pengujian terdata dan didokumentasikan dengan baik. 1.2 Laporan hasil uji coba konfigurasi pengamanan disetujui baik oleh pengguna dan pemegang kepentingan.
2. Mendukung desain dan pelaksanaan skenario latihan	1.1 Daftar risiko keamanan sistem informasi dan mitigasinya disusun. 1.2 Prosedur dan kebijakan pelaksanaan pelatihan dalam menghadapi risiko keamanan sistem informasi dibuat. 1.3 Laporan hasil pelatihan penanganan dalam menghadapi risiko keamanan sistem informasi dibuat.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

   2.2 Perlengkapan

   (Tidak ada.)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian
   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam melaksanakan uji coba konfigurasi pengamanan yang telah disesuaikan dengan rencana uji coba dan prosedur-prosedurnya. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:
   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.
   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.
   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
   3.1 Pengetahuan
      3.1.1 Standar yang berlaku terkait dengan keamanan informasi
      3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam membuat laporan hasil uji coba konfigurasi pengamanan disetujui baik oleh pengguna dan pemegang kepentingan

5.2 Ketepatan dalam membuat prosedur dan kebijakan pelaksanaan pelatihan dalam menghadapi risiko keamanan sistem informasi

5.3 Ketepatan dalam membuat laporan hasil pelatihan penanganan dalam menghadapi risiko keamanan sistem informasi

KODE UNIT : **J.62090.037.01**

JUDUL UNIT : **Mendeteksi Kerentanan (Vulnerabilitas) Keamanan dan Potensi Pelanggaran**

DESKRIPSI : Mengidentifikasi kerentanan keamanan yang dihasilkan dan mendeteksi potensi pelanggaran keamanan, mengambil tindakan yang sesuai untuk melaporkan kejadian tersebut sesuai dengan peraturan dan mengurangi dampak yang merugikan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mendeteksi potensi pelanggaran keamanan, mengambil tindakan yang sesuai untuk melaporkan kejadian tersebut sesuai dengan peraturan dan mengurangi dampak yang merugikan	1.1 Laporan deteksi potensi pelanggaran keamanan beserta tindakan pengamanan yang telah dilaksanakan dibuat.
2. Memeriksa seluruh potensi atas pelanggaran keamanan untuk menentukan apakah kebijakan lingkungan teknologi jaringan telah dilanggar, menganalisa dan mencatat seluruh dampak dan juga menjaga barang bukti	2.1 Daftar seluruh pelanggaran, hasil analisa, dan pencatatan dampak negatif yang terjadi dari adanya pelanggaran kebijakan disusun. 2.2 Jumlah potensi pelanggaran keamanan yang ada di dalam suatu sistem Teknologi Informasi diidentifikasi.
3. Mengidentifikasi kerentanan keamanan yang dari rencana implementasi atau kerentananyang tidak terdeteksi pada saat uji coba	3.1 Daftar potensi kerentanan keamanan yang sudah terdeteksi dalam fase uji coba maupun yang tidak terdeteksi dalam fase uji coba disusun. 3.2 Daftar kerentanan dan solusinya masing-masing disusun.
4. Melakukan tinjauan perlindungan keamanan tertentu untuk menentukan masalah keamanan (yang diidentifikasi dalam rencana yang telah disetujui) telah sepenuhnya ditangani	4.1 Laporan hasil kegiatan tinjauan perlindungan keamanan dibuat.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

   2.2 Perlengkapan

   (Tidak ada.)

3. Peraturan yang diperlukan

   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar

   4.1 Norma

   (Tidak ada.)

   4.2 Standar

   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam mengidentifikasi kerentanan keamanan yang dihasilkan dan mendeteksi potensi pelanggaran keamanan, mengambil tindakan yang sesuai untuk melaporkan kejadian tersebut sesuai dengan peraturan dan mengurangi

dampak yang merugikan. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Standar yang berlaku terkait dengan keamanan informasi

3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall*, IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam membuat laporan deteksi potensi pelanggaran keamanan beserta tindakan pengamanan yang telah dilaksanakan

5.2 Ketepatan dalam mengidentifikasi jumlah potensi pelanggaran keamanan yang ada di dalam suatu sistem teknologi informasi

5.3 Ketepatan dalam menyusun daftar kerentanan dan solusinya masing-masing

5.4 Ketepatan dalam membuat laporan hasil kegiatan tinjauan perlindungan keamanan

KODE UNIT : **J.62090.038.01**

JUDUL UNIT : **Melaksanakan Evaluasi Kelemahan (Vulnerabilitas) Keamanan**

DESKRIPSI : Melaksanakan koordinasi kegiatan pemeriksaan, pengujian dan tinjauan Keamanan Informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Melaksanakan koordinasi kegiatan pemeriksaan, tes, dan tinjauan keamanan dalam lingkungan jaringan sistem informasi	1.1 Rencana kerja kegiatan pemeriksaan, tes, dan tinjauan kegiatan keamanan pengelolaan sistem informasi disusun. 1.2 Laporan hasil kegiatan pemeriksaan, tes, dan tinjauan kegiatan keamanan pengelolaan sistem informasi dibuat.
2. Melacak dan melaporkan hasil tinjauan kegiatan pengelolaan sistem informasi	2.1 Rencana kerja kegiatan pemantauan dan tinjauan kegiatan pengelolaan sistem informasi disusun. 2.2 Laporan hasil kegiatan pemantuan dan tinjauan kegiatan pengelolaan sistem informasi dibuat.
3. Melakukan penilaian fisik keamanan jaringan sistem informasi dan melakukan koreksi atas kelemahan keamanan fisik jaringan sistem informasi	3.1 Rencana kegiatan penilaian keamanan jaringan sistem informasi disusun. 3.2 Laporan hasil kegiatan penilaian berupa fakta kerentanan/kelemahan keamanan jaringan sistem informasi dibuat. 3.3 Laporan hasil kegiatan koreksi kerentanan/kelemahan keamanan jaringan sistem informasi dibuat.
4. Memeriksa kerentanan posisi strategis dan menentukan tindakan untuk penanggulangannya	4.1 Daftar potensi kerentanan keamanan pada tingkatan strategis disusun. 4.2 Laporan hasil deteksi kerentanan dan solusi penanggulangannya dibuat.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya,

harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan
   2.1 Peralatan
   (Tidak ada.)
   2.2 Perlengkapan
   (Tidak ada.)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian
   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam melaksanakan koordinasi kegiatan pemeriksaan, pengujian dan tinjauan keamanan informasi. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:
   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.
   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.
   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

   3.1 Pengetahuan

      3.1.1 Standar yang berlaku terkait dengan keamanan informasi

      3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

      3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

      3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

   3.2 Keterampilan

      3.2.1 Mengoperasikan perangkat keras dan piranti lunak

      3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

      3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

   4.1 Disiplin

   4.2 Teliti

   4.3 Tanggung jawab

5. Aspek kritis

   5.1 Ketepatan dalam membuat laporan hasil kegiatan pemeriksaan, tes, dan tinjauan kegiatan keamanan pengelolaan sistem informasi

   5.2 Ketepatan dalam membuat laporan hasil kegiatan pemantuan dan tinjauan kegiatan pengelolaan sistem informasi

5.3 Ketepatan dalam membuat laporan hasil kegiatan penilaian berupa fakta kerentanan/kelemahan keamanan jaringan sistem informasi

5.4 Ketepatan dalam membuat laporan hasil kegiatan koreksi kerentanan/kelemahan keamanan jaringan sistem informasi

5.5 Ketepatan dalam membuat laporan hasil deteksi kerentanan dan solusi penanggulangannya

KODE UNIT : **J.62090.039.01**

JUDUL UNIT : **Mengimplementasikan Koreksi atas Kerentanan Keamanan Informasi**

DESKRIPSI : Mengimplementasikan koreksi atas segala kerentanan sistem yang bersifat teknis dan memberikan arahan dan/atau dukungan untuk para pengembang sistem mengenai pengkoreksian dari seluruh masalah keamanan data.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengimplementasikan koreksi atas segala kerentanan sistem yang bersifat teknis	1.1 Laporan hasil implementasi koreksi kerentanan yang ada dibuat. 1.2 Daftar tindakan korektif dan relevansinya terhadap penanganan kerentanan sistem disusun.
2. Memberikan arahan dan/atau dukungan untuk para pengembang sistem mengenai pengkoreksian dari seluruh masalah keamanan data yang teridentifikasi pada fase pengujian	2.1 Daftar potensi kerentanan keamanan yang sudah terdeteksi dalam fase uji coba maupun yang tidak terdeteksi dalam fase uji coba disusun. 2.2 Daftar kerentanan dan solusinya masing-masing disusun.
3. Mengimplementasi penanganan kerentanan dari sistem strategis	3.1 Prosedur dan kebijakan penanganan kerentanan keamanan informasi organisasi pada tingkatan strategis diidentifikasi. 3.2 *Log* insiden kerentanan keamanan pada tingkatan strategis dan solusinya dibuat.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan
   2.1 Peralatan
       (Tidak ada.)
   2.2 Perlengkapan
       (Tidak ada.)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
       (Tidak ada.)
   4.2 Standar
       4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam mengimplementasikan koreksi atas segala kerentanan sistem yang bersifat teknis dan memberikan arahan dan/atau dukungan untuk para pengembang sistem mengenai pengkoreksian dari seluruh masalah keamanan data. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.
   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.
   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

   3.1 Pengetahuan

      3.1.1 Standar yang berlaku terkait dengan keamanan informasi

      3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

      3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

      3.1.4 Pengetahuan dasar perlindungan informasi (*Backup* dan Enkripsi)

   3.2 Keterampilan

      3.2.1 Mengoperasikan perangkat keras dan piranti lunak

      3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

      3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

   4.1 Disiplin

   4.2 Teliti

   4.3 Tanggung jawab

5. Aspek kritis

   5.1 Ketepatan dalam mengidentifikasi prosedur dan kebijakan penanganan kerentanan keamanan informasi organisasi pada tingkatan strategis

   5.2 Ketepatan dalam membuat *log* insiden kerentanan keamanan pada tingkatan strategis dan solusinya

KODE UNIT : **J.62090.040.01**

JUDUL UNIT : **Mengelola Insiden Keamanan Informasi**

DESKRIPSI : Mengelola pelaksanaan prosedur dan tata cara pelaporan insiden yang berkaitan dengan insiden keamanan informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mematuhi prosedur terminasi sistem dan tata cara pelaporan insiden yang berkaitan dengan insiden keamanan atau serangan aktual terhadap infrastruktur dan penggunaan sistem teknologi informasi	1.1 Laporan kepatutan dan kepatuhan atas eksekusi terminasi sistem informasi dibuat. 1.2 *Log* catatan hasil insiden dan solusinya yang terjadi selama proses terminasi sistem dirangkum.
2. Mengawasi atau mengelola tindakan pengamanan atau perbaikan ketika suatu insiden keamanan atau kerentanan/kelemahan telah terjadi/ditemukan	2.1 Kebijakan dan prosedur manajemen insiden keamanan informasi telah disusun dan diaplikasikan. 2.2 Laporan hasil penanganan insiden keamanan informasi dibuat.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

   2.2 Perlengkapan

   (Tidak ada.)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian
   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam mengelola pelaksanaan prosedur dan tata cara pelaporan insiden yang berkaitan dengan insiden keamanan Informasi. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:
   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.
   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.
   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
   3.1 Pengetahuan
      3.1.1 Standar yang berlaku terkait dengan keamanan informasi
      3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam merangkum *log* catatan hasil insiden dan solusinya yang terjadi selama proses terminasi sistem

5.2 Ketepatan dalam membuat laporan hasil penanganan insiden keamanan informasi

KODE UNIT : **J.62090.041.01**

JUDUL UNIT : **Menyediakan Dukungan Keamanan untuk Permasalahan Perangkat Keras dan Piranti Lunak**

DESKRIPSI : Menyediakan dukungan, memonitor, menguji, dan memecahkan masalah perangkat keras dan masalah keamanan piranti lunak yang berkaitan dengan seluruh infrastruktur teknologi informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Memberikan dukungan, memonitor, menguji, dan memecahkan masalah perangkat keras dan masalah keamanan piranti lunak yang berkaitan dengan seluruh infrastruktur teknologi informasi	1.1 Laporan kegiatan dukungan pemecahan masalah keamanan yang berkaitan dengan seluruh infrastruktur teknologi informasi dibuat.
2. Memberikan dukungan, memonitor, menguji, dan memecahkan masalah perangkat keras dan masalah piranti lunak yang berkaitan dengan keamanan lingkungan jaringan	2.1 Prosedur operasi standar untuk acuan dukungan, pemantauan, dan pengujian masalah perangkat keras dan piranti lunak yang berkaitan dengan keamanan lingkungan diterapkan.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

   2.2 Perlengkapan

   (Tidak ada.)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian
   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam menyediakan dukungan, memonitor, menguji, dan memecahkan masalah perangkat keras dan masalah keamanan piranti lunak yang berkaitan dengan seluruh infrastruktur teknologi informasi. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:
   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.
   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.
   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
   3.1 Pengetahuan
      3.1.1 Standar yang berlaku terkait dengan keamanan informasi
      3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan

Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam membuat laporan kegiatan dukungan pemecahan masalah keamanan yang berkaitan dengan seluruh infrastruktur teknologi informasi

5.2 Ketepatan dalam menerapkan prosedur operasi standar untuk acuan dukungan, pemantauan, dan pengujian masalah perangkat keras dan piranti lunak yang berkaitan dengan keamanan lingkungan

KODE UNIT : **J.62090.042.01**

JUDUL UNIT : **Melakukan Aktifitas Penghapusan Hak Akses**

DESKRIPSI : Menghapus hak akses seluruh pegawai, kontraktor dan pengguna pihak ketiga terhadap informasi dan fasilitas pemrosesan informasi setelah pemberhentian pekerjaan, kontrak atau kesepakatan, atau penyesuaian karena adanya perubahan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi hak akses yang harus dihapuskan atau diubah	1.1 Hak akses yang telah diberikan kepada personil diidentifikasi. 1.2 Hak akses yang harus diubah atau dihapus terkait perubahan status personil diidentifikasi. 1.3 Perubahan hak akses pada sistem informasi diterapkan.
2. Melaksanakan penggantian *password*/akun yang diketahui oleh pegawai yang meninggalkan perusahaan, yang tetap aktif setelah pegawai tersebut keluar	2.1 *Password*/akun bersama yang juga diketahui oleh personil yang keluar diidentifikasi. 2.2 *Password*/akun, sesuai standar keamanan *password* organisasi, diganti. 2.3 *Password*/akun yang baru kepada anggota tim yang lain dipublikasikan.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

2.2 Perlengkapan

(Tidak ada.)

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam menghapus hak akses seluruh pegawai, kontraktor dan pengguna pihak ketiga terhadap informasi dan fasilitas pemrosesan informasi setelah pemberhentian pekerjaan, kontrak atau kesepakatan, atau penyesuaian karena adanya perubahan. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
    3.1 Pengetahuan
        3.1.1 Standar yang berlaku terkait dengan keamanan informasi
        3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)
        3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)
        3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)
    3.2 Keterampilan
        3.2.1 Mengoperasikan perangkat keras dan piranti lunak
        3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi
        3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan
    4.1 Disiplin
    4.2 Teliti
    4.3 Tanggung jawab

5. Aspek kritis
    5.1 Ketepatan dalam mengidentifikasi hak akses yang harus diubah atau dihapus terkait perubahan status personil
    5.2 Ketepatan dalam menerapkan perubahan hak akses pada sistem informasi

KODE UNIT : **J.62090.043.01**

JUDUL UNIT : **Mengimplementasikan Manajemen Perbaikan/Respon yang Terkait dengan Keamanan Informasi**

DESKRIPSI : Mendiagnosa dan menyelesaikan masalah keamanan dalam menanggapi insiden serta mengaplikasikan perbaikan yang terkait dengan keamanan informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Merekomendasikan dan menjadwalkan kegiatan perbaikan keamanan terkait di lingkungan jaringan	1.1 Daftar jadwal kegiatan perbaikan keamanan lingkungan jaringan disusun. 1.2 Daftar rekomendasi atas tindakan baik koreksi maupun pr*event*if dari ruang lingkup keamanan lingkungan jaringan disusun.
2. Melaksanakan kebijakan organisasi dan kebijakan *password* organisasi	2.1 Dokumen kebijakan penetapan *Password* dan penggunaannya diidentifikasi. 2.2 Laporan atas penerapan sistem *password* yang ada dibuat.
3. Bekerja dengan pengguna khusus lainnya untuk bersama-sama memecahkan masalah keamanan	3.1 *Log* catatan insiden dan solusinya dibuat. 3.2 Laporan kegiatan penanganan insiden keamanan informasi dibuat.
4. Mendiagnosa dan menyelesaikan masalah keamanan dalam menanggapi insiden yang telah dilaporkan	4.1 Prosedur dan kebijakan keamanan informasi organisasi yang terkait dengan penanganan insiden diidentifikasi. 4.2 *Log* catatan insiden dan solusinya dibuat.
5. Merekomendasikan jadwal dan/ataumenerapkan perbaikan yang terkait dengan keamanan dalam lingkungan daerah posisi strategis	5.1 Daftar layanan informasi beserta ketentuan keamanan informasi untuk tingkatan strategis disusun. 5.2 Rencana perbaikan keamanan informasi pada tingkatan strategis dibuat.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

   2.2 Perlengkapan

   (Tidak ada.)

3. Peraturan yang diperlukan

   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar

   4.1 Norma

   (Tidak ada.)

   4.2 Standar

   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam mendiagnosa dan menyelesaikan masalah keamanan dalam menanggapi insiden serta mengaplikasikan perbaikan yang terkait dengan keamanan informasi. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Standar yang berlaku terkait dengan keamanan informasi

3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam membuat laporan atas penerapan sistem *password* yang ada

5.2 Ketepatan dalam membuat *log* catatan insiden dan solusinya

KODE UNIT : **J.62090.044.01**

JUDUL UNIT : **Mengaplikasikan *Patch* Keamanan**

DESKRIPSI : Mengimplementasikan *patch* yang berlaku termasuk peringatan bahaya kerentanan keamanan, dokumentasi kerentanan keamanan dan pemberian saran teknis.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengimplementasikan *patch* yang berlaku termasuk peringatan bahaya kerentanan keamanan, dokumentasi kerentanan keamanan dan pemberikan saran teknis untuk lingkungan komputasi	1.1 *Patch* yang berlaku telah diaplikasikan pada lingkungan komputasi yang dipergunakan. 1.2 Butir-butir pokok yang terdapat pada dokumentasi kerentanan keamanan dideskripsikan. 1.3 Laporan kegiatan saran teknis yang telah dilaksanakan dibuat.
2. Menerapkan *patch* yang berlaku termasuk tanda kerentanan keamanan informasi, dan memberikan nasihat teknis untuk lingkungan jaringan yang mereka miliki	2.1 Rencana pemberlakuan *patch* disusun. 2.2 Daftar *patch* yang sudah diberlakukan dilaporkan.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

   2.2 Perlengkapan

   (Tidak ada.)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian
   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam mengimplementasikan *patch* yang berlaku termasuk peringatan bahaya kerentanan keamanan, dokumentasi kerentanan keamanan dan pemberian saran teknis. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:
   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.
   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.
   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
   3.1 Pengetahuan
      3.1.1 Standar yang berlaku terkait dengan keamanan informasi
      3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan

Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam mempergunakan *patch* yang berlaku telah diaplikasikan pada lingkungan komputasi

5.2 Ketepatan dalam membuat laporan kegiatan saran teknis yang telah dilaksanakan

KODE UNIT : **J.62090.045.01**

JUDUL UNIT : **Mengelola Integritas Informasi**

DESKRIPSI : Mengelola integritas informasi yang tersedia dalam sistem yang tersedia dan melindungi untuk mencegah pengubahan tanpa otorisasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menetapkan mekanisme perlindungan terhadap *software*, data, dan informasi lainnya yang tersedia	1.1 Mekanisme kontrol untuk memenuhi perubahan terkait dengan *software*, data dan informasi lainnya yang tersedia diimplementasikan. 1.2 Data yang relevan dalam suatu koleksi informasi dikumpulkan. 1.3 Informasi pribadi hanya akan digunakan atau diungkapkan untuk keperluan yang sesuai tujuan pemberian informasi kecuali atas dasar persetujuan pribadi diimplementasikan. 1.4 Langkah-langkah yang tepat diambil untuk perlindungan data didefinisikan. 1.5 Prosedur-prosedur untuk menjaga *software*, data dan informasi diakses oleh pihak-pihak tertentu ditetapkan.
2. Menetapkan mekanisme persetujuan sebelum suatu informasi diberikan kepada pihak lain	2.1 Informasi yang bertentangan diperiksa dan kebutuhan yang tepat ditetapkan. 2.2 Persetujuan diakses oleh pihak-pihak terkait.
3. Melaksanakan kontrol terhadap sistem publikasi secara elektronik	3.1 Sistem publikasi disosialisasikan. 3.2 Revisi dan penyempurnaan publikasi dilaksanakan sesuai kebutuhan dilaksanakan.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

2.1 Peralatan

(Tidak ada.)

2.2 Perlengkapan

(Tidak ada.)

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam mengelola integritas informasi yang tersedia dalam sistem yang tersedia dan melindungi untuk mencegah pengubahan tanpa otorisasi. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
    3.1 Pengetahuan
        3.1.1 Standar yang berlaku terkait dengan keamanan informasi
        3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)
        3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)
        3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)
    3.2 Keterampilan
        3.2.1 Mengoperasikan perangkat keras dan piranti lunak
        3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi
        3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan
    4.1 Disiplin
    4.2 Teliti
    4.3 Tanggung jawab

5. Aspek kritis
    5.1 Ketepatan dalam mengimplementasikan mekanisme kontrol untuk memenuhi perubahan terkait dengan *software*, data dan informasi lainnya yang tersedia
    5.2 Ketepatan dalam menetapkan informasi yang bertentangan diperiksa dan kebutuhan yang tepat

KODE UNIT : **J.62090.046.01**

JUDUL UNIT : **Mengelola Penggunaan Media Penyimpanan Sementara (*Removable Media*)**

DESKRIPSI : Menetapkan dan melaksanakan prosedur untuk pengelolaan penyimpanan sementara (*removable media*). Proses pembuangan/penghancuran media dilakukan secara aman dan tepat ketika media tersebut tidak lagi dibutuhkan, dan dengan menggunakan prosedur formal.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengelola penggunaan media penyimpanan sementara	1.1 Kriteria dari media penyimpanan didefinisikan. 1.2 Isi dari media yang tidak lagi digunakan dihapus, media dibuang dan dibuat agar tidak dapat di *recover*. 1.3 Otorisasi untuk pembuangan media dari organisasi dan pencatatan dari penghapusan ini agar dapat dikelola pada saat audit disimpan. 1.4 Semua media harus disimpan dalam lingkungan yang aman dan terjamin sesuai dengan spesifikasi yang ditentukan oleh pabrik pembuatnya. 1.5 Informasi yang disimpan dalam media harus juga disimpan ditempat lain agar menghindari kehilangan informasi yang disebabkan kerusakan media. 1.6 Registrasi dari media penyimpanan ditetapkan pada batasan kemungkinan terjadinya kehilangan data.
2. Menentukan penyimpanan dan pembuangan media yang mengandung informasi yang penting secara aman dan tepat	2.1 Tipe utama dari modifikasi sistem diidentifikasi, meliputi koreksi kesalahan, perbaikan sistem, bantuan dan pengembangan. 2.2 Keberadaan tempat penyimpanan, meliputi penyimpanan pusat, pustaka program, dan basis data dikonfirmasikan.
3. Menerapkan prosedur untuk mengidentifikasi barang yang harus dibuang secara aman	3.1 Formulir permintaan pembuangan dan tingkat otoritas yang diperlukan disiapkan atau diperiksa. 3.2 Strategi *back-up* dan penghapusan ditetapkan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
4. Mencatat kegiatan pembuangan barang-barang penting sehingga mempermudah dalam mengelola proses audit	4.1 Laporan terkait perubahan dan pembuangan disampaikan kepada pihak yang terkait dibuat. 4.2 Semua dokumentasi dan tempat penyimpanan diperbaharui dan diamandemen.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan
   - 2.1 Peralatan

     (Tidak ada.)
   - 2.2 Perlengkapan

     (Tidak ada.)

3. Peraturan yang diperlukan
   - 3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   - 3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   - 4.1 Norma

     (Tidak ada.)
   - 4.2 Standar

     4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam menetapkan dan melaksanakan prosedur untuk pengelolaan penyimpanan sementara (*removable media*). Proses pembuangan/penghancuran media dilakukan secara aman dan tepat ketika media tersebut tidak lagi dibutuhkan, dan dengan menggunakan prosedur formal. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.

   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.

   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

   3.1 Pengetahuan

      3.1.1 Standar yang berlaku terkait dengan keamanan informasi

      3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

      3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

      3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

   3.2 Keterampilan

      3.2.1 Mengoperasikan perangkat keras dan piranti lunak

      3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

      3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan
    4.1 Disiplin
    4.2 Teliti
    4.3 Tanggung jawab

5. Aspek kritis
    5.1 Ketepatan dalam menyiapkan atau memeriksa formulir permintaan pembuangan dan tingkat otoritas yang diperlukan
    5.2 Ketepatan dalam membuat laporan terkait perubahan dan pembuangan disampaikan kepada pihak yang terkait
    5.3 Ketepatan dalam memperbaharui dan mengamandemen semua dokumentasi dan tempat penyimpanan

KODE UNIT : **J.62090.047.01**

JUDUL UNIT : **Merancang dan Mengelola Sistem *Backup***

DESKRIPSI : Merancang dan mengelola sistem *backup* untuk menjamin keberlangsungan sistem setelah bencana.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mendefinisikan tingkat *backup* informasi yang diperlukan	1.1 Persyaratan bisnis terhadap informasi, termasuk jangka waktu ketersediaan, tingkat kepentingan, dan lain-lain diidentifikasi. 1.2 Tingkat *backup* yang diperlukan masing-masing tipe informasi ditetapkan. 1.3 Kesesuaian tipe *backup* (*full*, *incremental*, atau lainnya) serta frekuensi *backup* dengan kebutuhan bisnis dan persyaratan informasi yang terkait, serta tingkat kegunaan informasi terhadap keberlanjutan operasional organisasi dianalisa.
2. Merancang fasilitas *backup* yang memadai untuk memastikan seluruh informasi dan *software* yang penting dapat tersedia kembali setelah bencana atau kerusakan media	2.1 Informasi dan *software* yang perlu di *backup* diidentifikasi. 2.2 Kapasitas *backup* yang diperlukan, dengan mempertimbangkan waktu yang diperlukan untuk menyimpan informasi tersebut dikalkulasi. 2.3 Sistem *backup* sesuai standar pemulihan terhadap bencana dan persyaratan keberlanjutan bisnis disiapkan. 2.4 Prosedur dan penjadwalan backup ditetapkan.
3. Memilih lokasi untuk fasilitas *backup* informasi di jarak yang aman, untuk menghindari kerusakan yang bersamaan dengan situs utama	3.1 Wilayah sekitar lokasi utama, yang memiliki profil bencana dan musibah yang sama dengan lokasi utama diidentifikasi. 3.2 Lokasi *backup* diluar wilayah tersebut ditentukan.
4. Menerapkan perlindungan fisik dan lingkungan kepada informasi *backup* yang sesuai dengan standar yang diterapkan pada lokasi utama	4.1 Persyaratan keamanan fisik lokasi *backup* yang sama dengan lokasi utama diidentifikasi. 4.2 Prosedur dan pengendalian untuk mencapai persyaratan keamanan fisik diterapkan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
5. Menerapkan enkripsi pada informasi *backup* sesuai kebutuhan	5.1 Persyaratan keamanan bagi masing-masing informasi *backup*, terutama terkait kerahasiaan diidentifikasi. 5.2 Teknologi enkripsi yang sesuai diterapkan, dengan memperimbangkan kemampuan fasilitas pemrosesan informasi.
6. Menentukan jangka waktu penyimpanan informasi *backup* sesuai kebutuhan bisnis	6.1 Persyaratan bisnis untuk periode penyimpanan informasi *backup* diidentifikasi. 6.2 Kapasitas sistem yang dibutuhkan untuk menyimpan informasi *backup* ditentukan.
7. Mengelola administrasi *backup*	7.1 Catatan yang lengkap dan akurat mengenai *backup* yang tersedia disusun. 7.2 Prosedur restorasi informasi *backup* didokumentasikan.
8. Melakukan pengujian secara berkala kepada media *backup* untuk memastikan media tersebut dapat diandalkan pada kondisi darurat	8.1 Jadwal dan prosedur pengujian ditentukan. 8.2 Media *backup* dipersiapkan sehingga siap untuk diuji pada kondisi yang sesuai. 8.3 Kesesuaian informasi *backup* dengan informasi utama diuji.
9. Melakukan pengujian secara berkala terhadap prosedur restorasi, untuk memastikan bahwa prosedur tersebut efektif dan dapat dilakukan pada jangka waktu yang dialokasikan oleh prosedur pemulihan	9.1 Jadwal dan prosedur pengujian restorasi ditentukan. 9.2 Media *backup* dipersiapkan untuk diuji pada kondisi yang sesuai. 9.3 Prosedur restorasi dilaksanakan. 9.4 Efektivitas dan keakuratan prosedur restorasi dianalisa.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya,

harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan
   2.1 Peralatan
       (Tidak ada.)
   2.2 Perlengkapan
       (Tidak ada.)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
       (Tidak ada.)
   4.2 Standar
       4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian

   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam merancang dan mengelola sistem *backup* untuk menjamin keberlangsungan sistem setelah bencana. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:

   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.
   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.
   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

   3.1 Pengetahuan

      3.1.1 Standar yang berlaku terkait dengan keamanan informasi

      3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

      3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

      3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

   3.2 Keterampilan

      3.2.1 Mengoperasikan perangkat keras dan piranti lunak

      3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

      3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

   4.1 Disiplin

   4.2 Teliti

   4.3 Tanggung jawab

5. Aspek kritis

   5.1 Ketepatan dalam mengidentifikasi persyaratan bisnis untuk periode penyimpanan informasi *backup* dan menentukan kapasitas sistem yang dibutuhkan untuk menyimpan informasi *backup*

   5.2 Ketepatan dalam menyusun catatan yang lengkap dan akurat mengenai *backup* yang tersedia

KODE UNIT : **J.62090.048.01**

JUDUL UNIT : **Melaksanakan Kegiatan Pemulihan Data**

DESKRIPSI : Melaksanakan proses pemulihan data yang diakibatkan oleh berbagai gangguan dan kerusakan data dan jaringan sistem informasi yang dikelola serta melaksanakan kegiatan yang diperlukan untuk menjaga integritas data.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Memberikan dukungan dan mengelola retensi dan pemulihan data dalam lingkungan komputasi	1.1 Butir-butir pokok yang terdapat pada prosedur pengelolaan retensi dan pemulihan data dideskripsikan. 1.2 Laporan insiden yang terkait dengan retensi dan pemulihan data dibuat.
2. Memonitor proses pemulihan jaringan sistem informasi dan memulihkan kembali fitur keamanan dan prosedur untuk keamanan jaringan sistem informasi	2.1 Jaringan sistem informasi yang terganggu telah dipulihkan kembali ke keadaan normal. 2.2 Fitur keamanan dan prosedur keamanan telah diterapkan. 2.3 Laporan hasil pemulihan jaringan sistem informasi dibuat.

BATASAN VARIABEL

1. Konteks variabel

   Unit kompetensi ini berlaku untuk menjelaskan prinsip keamanan informasi secara umum. SDM yang bertanggung jawab menjalankan fungsi ini, terlepas dari apapun peran dan jabatan dari organisasinya, harus bisa diidentifikasikan sebagai SDM keamanan informasi dan harus patuh melaksanakan butir-butir elemen kompetensi yang terkait.

2. Peralatan dan perlengkapan

   2.1 Peralatan

   (Tidak ada.)

   2.2 Perlengkapan

   (Tidak ada.)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
   4.2.1 *Standar Operating Procedure* (SOP)

PANDUAN PENILAIAN

1. Konteks penilaian
   Unit kompetensi ini dinilai berdasarkan tingkat kemampuan dalam melaksanakan proses pemulihan data yang diakibatkan oleh berbagai gangguan dan kerusakan data dan jaringan sistem informasi yang dikelola serta melaksanakan kegiatan yang diperlukan untuk menjaga integritas data. Penilaian dapat dilakukan di Tempat Uji Kompetensi (TUK) dengan cara:
   1.1 Wawancara mengacu kepada Kriteria Unjuk Kerja.
   1.2 Demonstrasi secara konseptual dalam rangka aktualisasi pelaksanaan pekerjaan.
   1.3 Metode-metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
   3.1 Pengetahuan
      3.1.1 Standar yang berlaku terkait dengan keamanan informasi
      3.1.2 Pengetahuan dasar tentang Konsep Dasar Keamanan Informasi (Pengelolaan Risiko; Ketersediaan, Integritas dan

Kerahasiaan; Orang, Proses dan Teknologi; Keamanan Fisik)

3.1.3 Pengetahuan dasar tentang Teknologi Keamanan Informasi Fundamental (Kontrol Akses, *Patch Management*, Anti *Malware*, Anti *Spam*, *Firewall,* IPS)

3.1.4 Pengetahuan dasar Perlindungan Informasi (*Backup* dan Enkripsi)

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat keras dan piranti lunak

3.2.2 Mengaplikasikan petunjuk konfigurasi keamanan sistem konfigurasi

3.2.3 Mampu mendeteksi potensi pelanggaran keamanan

4. Sikap yang dibutuhkan

4.1 Disiplin

4.2 Teliti

4.3 Tanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam membuat laporan insiden yang terkait dengan retensi dan pemulihan data

5.2 Ketepatan dalam membuat laporan hasil pemulihan jaringan sistem informasi

BAB III

KETENTUAN PENUTUP

Dengan ditetapkannya Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Kegiatan Pemrograman, Konsultasi Komputer dan Kegiatan ybdi Bidang Keamanan Informasi maka SKKNI ini berlaku secara nasional dan menjadi acuan bagi penyelenggaraan pendidikan dan pelatihan profesi, uji kompetensi dan sertifikasi profesi.

Ditetapkan di Jakarta
pada tanggal 24 Februari 2015

MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA,

KETENAGAKERJAAN R.I. MENTERI

M. HANIF DHAKIRI