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);

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.62090.015.01**

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.62090.022.01**

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.62090.037.01**

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.62090.039.01**

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