BNSP
BADAN NASIONAL SERTIFIKASI PROFESI

LSP T.U.K PANDUNET

Panduan Uji Kompetensi

Skema Sertifikasi Junior Cyber Security

Daftar Isi

1. Latar Belakang

Sertifikasi profesi merupakan upaya untuk memberikan pengakuan atas kompetensi yang dikuasai seseorang sesuai dengan Standard Kompetensi Kerja Nasional Indonesia (SKKNI), standar internasional atau standar khusus. Standar Kompetensi adalah pernyataan yang menguraikan keterampilan, pengetahuan dan sikap yang harus dilakukan saat bekerja serta penerapannya, sesuai dengan persyaratan yang ditetapkan oleh tempat kerja (industri).

Kompeten diartikan kemampuan dan kewenangan yang dimiliki oleh seseorang untuk melakukan suatu pekerjaan yang didasari oleh pengetahuan, ketrampilan dan sikap sesuai dengan unjuk kerja yang ditetapkan. Sertifikasi dilaksanakan dengan uji kompetensi melalui beberapa metode uji oleh asesor yang dimiliki lisensi dari BNSP. Uji kompetensi dilaksanakan di Tempat Uji Kompetensi (TUK). TUK LSP TIK Indonesia merupakan tempat kerja atau lembaga yang dapat memberikan fasilitas pelaksanaan uji kompetensi yang telah diverifikasikan oleh LSP TIK Indonesia.

2. Persyaratan Dasar Pemohon Sertifikasi

2.1. Minimal telah menyelesaikan pendidikan Diploma Satu (D1); Atau

2.2. Memiliki sertifikat pelatihan berbasis kompetensi yang sesuai dengan Skema Sertifikasi Junior Cyber Security; Atau

2.3. Telah berpengalaman kerja pada lingkup yang sesuai dengan Skema Sertifikasi Junior Cyber Security minimal 1 tahun secara berkelanjutan;

3. Hak Pemohon Sertifikasi dan Kewajiban Pemegang Sertifikat

3.1. Hak Pemohon

- 3.1.1. Memperoleh penjelasan tentang gambaran proses sertifikasi sesuai dengan skema sertifikasi.
- 3.1.2. Mendapatkan hak bertanya berkaitan dengan kompetensi.
- 3.1.3. Memperoleh pemberitahuan tentang kesempatan untuk menyatakan, dengan alasan, permintaan untuk disediakan kebutuhan khusus sepanjang integritas asesmen tidak dilanggar, serta mempertimbangkan aturan yang bersifat Nasional.
- 3.1.4. Memperoleh hak banding terhadap keputusan Sertifikasi.
- 3.1.5. Memperoleh sertifikat kompetensi jika dinyatakan kompeten.
- 3.1.6. Menggunakan sertifikat untuk promosi diri sebagai ahli dalam Skema Sertifikasi Junior Cyber Security.

3.2. Kewajiban Pemegang Sertifikat

- 3.2.1. Melaksanakan keprofesian sesuai dengan Skema Sertifikasi Junior Cyber Security.
- 3.2.2. Menjaga dan mentaati kode etik profesi secara sungguh-sungguh dan konsekuen.
- 3.2.3. Menjamin bahwa sertifikat kompetensi tidak disalahgunakan.
- 3.2.4. Menjamin terpelihara kompetensi yang sesuai dengan sertifikat kompetensi.
- 3.2.5. Menjamin bahwa seluruh pernyataan dan informasi yang diberikan adalah terbaru, benar dan dapat dipertanggung jawabkan.

3.2.6. Melaporkan rekaman kegiatan yang sesuai Skema Sertifikasi Junior Cyber Security setiap 6 bulan sekali.

3.2.7. Membayar biaya sertifikasi.

4. Persyaratan Sertifikasi

Peserta uji kompetensi harus melengkapi persyaratan yang sesuai dengan Skema Sertifikasi Junior Cyber Securityyang meliputi:

4.1. Melengkapi isian formulir permohonan (FR-APL01) dan formulir asesmen mandiri (FR-APL02)

4.2. Menyerahkan persyaratan uji kompetensi

a. Pas foto 3x4 (3 lembar).
b. Copy identitas diri KTP/KK (1 lembar).
c. Copy ijazah terakhir (1 lembar).
d. Copy sertifikat yang relevan dengan Skema Sertifikasi Junior Cyber Security, bila ada.
e. CV pengalaman / keterangan kerja yang relevan dengan Skema Sertifikasi Junior Cyber Security, bila ada.
f. Portofolio yang relevan dengan Skema Sertifikasi Junior Cyber Security, bila ada.

5. Proses Sertifikasi

5.1. Calon peserta uji kompetensi mengajukan permohonan sertifikasi melalui TUK (Tempat Uji Kompetensi) yang telah diverifikasi oleh LSP TIK Indonesia atau langsung melalui LSP TIK Indonesia.

5.2. Calon peserta uji kompetensi melengkapi isian formulir permohonan (FR-APL01) dan formulir asesmen mandiri (FR-APL02) serta menyerahkan persyaratan uji kompetensi.

5.3. Calon peserta uji kompetensi akan disetujui sebagai peserta uji kompetensi apabila persyaratan dan bukti-bukti yang disertakan telah memadai sesuai dengan skema sertifikasi.

5.4. Asesor dan peserta uji kompetensi menentukan tempat dan waktu pelaksanaan uji kompetensi yang telah disepakati oleh kedua belah pihak.

5.5. Setelah proses uji kompetensi, Asesor merekomendasikan kompeten (K) atau belum kompeten(BK) berdasarkan bukti-bukti yang telah dikumpulkan selama proses uji kompetensi.

5.6. LSP TIK Indonesia mengadakan rapat pleno untuk memberikan keputusan hasil uji kompetensi berdasarkan rekomendasi dari Asesor Kompetensi dan bukti-bukti yang telah dikumpulkan selama proses uji kompetensi.

5.7. LSP TIK Indonesia menerbitkan Sertifikat Kompetensi Skema Sertifikasi Junior Cyber Security bagi peserta uji kompetensi yang dinyatakan **Kompeten** di semua unit kompetensi yang diujikan.

5.8. LSP TIK Indonesia menerbitkan Surat Keterangan telah mengikuti proses uji kompetensi bagi peserta uji kompetensi yang dinyatakan **Belum Kompeten**.

6. Rincian Unit Kompetensi

No	Kode Unit	Judul Unit
1	J.62090.001.01	Menerapkan prinsip perlindungan informasi
2	J.62090.003.01	Menerapkan prinsip keamanan informasi untuk penggunaan jaringan internet
3	J.62090.004.01	Menerapkan prinsip keamanan informasi pada transaksi elektronik
4	J.62090.006.01	Melaksanakan kebijakan keamanan informasi
5	J.62090.012.01	Mengaplikasikan ketentuan/persyaratan keamanan informasi
6	J.62090.020.01	Mengelola log
7	J.62090.032.01	Menerapkan kontrol akses berdasarkan konsep/metodologi yang telah ditetapkan

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.
5. Mengumpulkan dan memelihara data yang diperlukan untuk memenuhi persyaratan pelaporan keamanan sistem	5.1. Data yang diperlukan untuk memenuhi persyaratan pelaporan keamanan system dideskripsikan. 5.2. Laporan berkala keamanan sistem dibuat.

Kode Unit : **J.62090.003.01**
Judul Unit : **Menerapkan Prinsip Keamanan Informasi untuk Penggunaan Jaringan Internet**
Deskripsi Unit : 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 jenisjenis 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.

Kode Unit : **J.62090.004.01**
Judul Unit : **Menerapkan Prinsip Keamanan Informasi pada Transaksi Elektronik**
Deskripsi Unit : 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 pihakpihak yang terlibat dievaluasi 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.

Kode Unit : **J.62090.006.01**
Judul Unit : **Melaksanakan Kebijakan Keamanan Informasi**
Deskripsi Unit : 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.

Kode Unit : **J.62090.012.01**
Judul Unit : **Mengaplikasikan Ketentuan/Persyaratan Keamanan Informasi**
Deskripsi Unit : 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/system keamanan yang telah diterapkan.
2. Menyediakan masukan tentang hal yang terkait dengan persyaratan	2.1. Daftar persyaratan keamanan yang akan dimasukan dalam dokumen pengadaan telah disusun.

keamanan untuk dimasukkan dalam laporan pekerjaan dan dokumen - dokumen pengadaan terkait	
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. 5.2. Persyaratan keamanan untuk perangkat keras, piranti lunak, da 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 analis persyaratan keamanan yang relevan terhadap kemampuan teknologi informasi yang baru dibuat

Kode Unit : **J.62090.020.01**
Judul Unit : **Mengelola *Log***
Deskripsi Unit : 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	3.1. Kebutuhan kapasitas media penyimpanan file pencatatan dianalisa.

pencatatan terhadap kemungkinan penuh sehingga terjadi kegagalan ketika mencatat kejadian yang terjadi	3.2. Alokasi kapasitas disediakan agar mencegah terjadinya kegagalan tersebut.

Kode Unit : **J.62090.032.01**

Judul Unit : **Menerapkan Kontrol Akses Berdasarkan Konsep/Metodologi yang telah Ditetapkan**

Deskripsi Unit : 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 system 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.
6. Melakukan kontrol dan pengawasan pada setiap pengguna yang memiliki akses khusus menjalankan fungsi keamanan agar menerima pelatihan	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

keamanan dasar dan berkelanjutan serta mendapatkan sertifikasi yang sesuai untuk melaksanakan tugas keamanan	