LSP
LEMBAGA SERTIFIKASI PROFESI
TELEKOMUNIKASI DIGITAL INDONESIA

SKEMA SERTIFIKASI OKUPASI
Cybersecurity Analyst / Cybersecurity Incident Analyst

BNSP

BADAN NASIONAL SERTIFIKASI PROFESI

LEMBAR VERIFIKASI

Nama LSP	:	TELEKOMUNIKASI DIGITAL INDONESIA
Nama Skema	:	Cybersecurity Analyst / Cyberfsecurity Incident Analyst
Jenis Skema	:	Okupasi
Diverifikasi Tanggal	:	24 Oktober 2023

Verifikator

Inda Mapilindari

Komisioner
Koordinator Lisensi

Mulyanto

Wakil Ketua
Selaku Ketua Tim Verifikator

Miftakul Azis, MH

2023

SKEMA SERTIFIKASI OKUPASI
Cybersecurity Analyst /
Cybersecurity Incident Analyst

Skema sertifikasi Okupasi **Cybersecurity Analyst / Cybersecurity Incident Analyst** adalah skema sertifikasi Okupasi yang dikembangkan oleh Komite Skema Lembaga Sertifikasi Profesi (LSP) Telekomunikasi Digital Indonesia (LSP TDI) untuk memenuhi kebutuhan sertifikasi kompetensi kerja di LSP Telekomunikasi Digital Indonesia (LSP TDI). Kemasan yang digunakan mengacu pada Standar Kompetensi Kerja Nasional Indonesia berdasarkan 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, dan Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber Tahun 2019 Nomor : 563.1 Tahun 2019 yang disahkan tanggal 12 Desember 2019. Skema sertifikasi ini digunakan sebagai acuan pada pelaksanaan assesmen oleh Asesor kompetensi LSP Telekomunikasi Digital Indonesia (LSP TDI) dan memastikan kompetensi pada jabatan **Cybersecurity Analyst / Cybersecurity Incident Analyst.**

Disahkan tanggal : 16 Oktober 2023
Oleh :

Lingga Wardhana	Wiryandaru Restiawan
Ketua LSP	Ketua Komite Skema LSP
Telekomunikasi Digital Indonesia	Telekomunikasi Digital Indonesia

Nomor Dokumen : SKEMA-23/ Cybersecurity Analyst / Cybersecurity Incident Analyst
Nomor Salinan : 01
Status Distribusi :

- [v] Terkendali
- [ ] Tak Terkendali

1. Latar Belakang

1.1. Disusun guna memenuhi peraturan perundangan yang menyatakan bahwa setiap tenaga kerja berhak mendapatkan pengakuan kompetensi yang dimilikinya yang diperoleh melalui pendidikan, pelatihan dan pengalaman kerja dan pemenuhan peraturan tentang sertifikasi kompetensi SDM sektor Teknologi Informasi sub sektor Keamanan Informasi.

1.2. Disusun dalam rangka memenuhi kebutuhan tenaga kerja kompeten di sektor Teknologi Informasi sub sektor Keamanan Informasi yang banyak dibutuhkan pada saat inidan masa yang akan datang.

1.3. Disusun untuk memenuhi kebutuhan sertifikasi kompetensi oleh LSP Telekomunikasi Digital Indonesia.

1.4. Skema sertifikasi ini diharapkan menjadi acuan pengembangan pendidikan dan pelatihan berbasis kompetensi.

1.5. Dalam rangka meningkatkan daya saing tenaga kerja di pasar kerja regional, nasional dan internasional di sektor Teknologi Informasi sub sektor Keamanan Informasi.

2. Ruang Lingkup Skema Sertifikasi

2.1. Ruang Lingkup pengguna hasil sertifikasi kompetensi ini meliputi peluang kerja di sektor Teknologi Informasi sub sektor Keamanan Informasi.

2.2. Lingkup isi skema ini meliputi sejumlah unit kompetensi yang dilakukan uji kompetensi guna memenuhi kompetensi pada jabatan Cybersecurity Analyst / Cybersecurity Incident Analyst.

3. Tujuan Sertifikasi

3.1. Memastikan kompetensi kerja pada jabatan Cybersecurity Analyst / Cybersecurity Incident Analyst.

3.2. Sebagai acuan bagi LSP Telekomunikasi Digital Indonesia dan asesor dalam rangka pelaksanaan sertifikasi kompetensi.

4. Acuan Normatif

4.1. Undang-Undang Republik Indonesia Nomor 13 Tahun 2003 Tentang Ketenagakerjaan.

4.2. Undang-Undang RepublikIndonesia Nomor 3 Tahun 2014 Tentang Perindustrian.

4.3. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

4.4. Peraturan Pemerintah Republik Indonesia Nomor 31 Tahun 2006 Tentang Sistem Pelatihan Kerja Nasional.

4.5. Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012 Tentang Penyelenggaran Sistem dan Transaksi Elektronik

4.6. Peraturan Presiden Republik Indonesia Nomor 8 Tahun 2012 tentang Kerangka Kualifikasi Nasional Indonesia.

4.7. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 24 Tahun 2015 tentang Pemberlakuan Standar Kompetensi Kerja Nasional Indonesia Bidang Komunikasi dan Informatika.

4.8. 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.

4.9. Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber Tahun 2019 Nomor : 563.1 Tahun 2019 yang disahkan tanggal 12 Desember 2019.

4.10. Peraturan Badan Nasional Sertifikasi Profesi Nomor 2/BNSP/VIII/2017 Tahun 2017 tentang Pedoman Pengembangan dan Pemeliharan Skema Sertifikasi Profesi.

5. Kemasan / Paket Kompetensi

5.1 Jenis Skema : ~~KKNI~~ / Okupasi / ~~Klaster~~

5.2 Nama Skema : Cybersecurity Analyst / Cybersecurity Incident Analyst (Jenjang Kualifikasi 6)

Rincian Unit Kompetensi :

NO	KODE UNIT	JUDUL UNIT KOMPETENSI
1.	J.62090.015.01	Melaksanakan Koordinasi dan Pengarahan Pelaksanaan Tugas-Tugas Keamanan Informasi
2.	J.62090.037.01	Mendeteksi Kerentanan (Vulnerabilitas) Keamanan dan Potensi Pelanggaran
3.	J.62090.039.01	Mengimplementasikan Koreksi Atas Kerentanan Keamanan Informasi
4.	J.62090.008.01	Melaksanakan Ketentuan Hukum yang Berlaku tentang Keamanan Informasi
5.	J.62090.016.01	Mengelola SDM yang Terkait dengan Tugas-Tugas Keamanan Informasi
6.	J.62090.022.01	Melakukan Evaluasi Kinerja Keamanan Informasi

6. Persyaratan Dasar Pemohon Sertifikasi

6.1. Memiliki ijazah minimal D4 atau S1 Teknik Informatika, atau Teknik Elektro atau Teknik Komputer, atau Teknik Telekomunikasi; atau

6.2. Memiliki ijazah minimal D4 atau D1 dan telah mengikuti pelatihan berbasis kompetensi *Cybersecurity Analyst / Cybersecurity Incident Analyst*; atau

6.3. Telah berpengalaman kerja sebagai *Junior Cyber Security, Cyber Security Specialist* dengan pengalaman minimal 3 tahun di jabatan tersebut; atau

Verified BNSP

6.4. Telah berpengalaman kerja sebagai *Cybersecurity Analyst / Cybersecurity Incident Analyst* dengan pengalaman minimal 2 tahun di jabatan tersebut.

7. Hak Pemohon Sertifikasi dan Kewajiban Pemegang Sertifikat

7.1. Hak Pemohon

7.1.1. Memperoleh penjelasan tentang gambaran proses sertifikasi sesuai dengan skema sertifikasi.
7.1.2. Mendapatkan hak bertanya berkaitan dengan kompetensi.
7.1.3. Memperoleh jaminan kerahasiaan atas proses sertifikasi.
7.1.4. Memperoleh hak banding terhadap keputusan sertifikasi.
7.1.5. Memperoleh sertifikat kompetensi jika dinyatakan kompeten.
7.1.6. Menggunakan untuk promosi diri sebagai profesi bidang Cybersecurity Analyst / Cybersecurity Incident Analyst.

7.2. Kewajiban Pemegang Sertifikat

7.2.1. Menjamin bahwa sertifikat kompetensi tidak disalahgunakan.
7.2.2. Menjamin terpeliharanya kompetensi yang sesuai pada sertifikat kompetensi.
7.2.3. Menjamin bahwa seluruh pernyataan dan informasi yang diberikan adalah terbaru, benar dan dapat dipertanggung jawabkan.
7.2.4. Menjamin mentaati aturan penggunaan sertifikat.

8. Biaya Sertifikasi

8.1 Biaya sertifikasi Cybersecurity Analyst / Cybersecurity Incident Analyst sebesar Rp 2.500.000,- (Dua juta lima ratus ribu rupiah).

9. Proses Sertifikasi

9.1. Proses Pendaftaran

LSP menginformasikan kepada pemohon persyaratan sertifikasi sesuai skema sertifikasi, jenis bukti, aturan bukti, proses sertifikasi, hak pemegang sertifikat kompetensi.

9.1.1. LSPTelekomunikasi Digital Indonesia (LDP TDI) menginformasikan kepada pemohon persyaratan sertifikasi sesuai skema sertifikasi jenis bukti, aturan, aturan bukti, proses sertifikasi, hak pemohonan dan kewajibanpemohon, biaya sertifikasi dan kewajiban pemegang
9.1.2. Pemohon mengisi formulir Permohonan Sertifikasi (APL 01) yang dilengkapi dengan bukti :
   a. Pas foto 3x4
   b. Foto copy KTP
   c. Daftar Riwayat Hidup (CV)
   d. Copy ijazah minimal D4 atau S1 Teknik Informatika, atau Teknik Elektro atau Teknik Komputer, atau Teknik Telekomunikasi; atau
   e. Copy ijazah minimal D4 atau S1 dan Sertifikat Pelatihan berbasis

kompetensi *CybersecurityAnalyst / Cybersecurity Incident Analyst; atau*

f. Copy Surat Keterangan Kerja sebagai *Junior Cyber Security* atau *Cyber Security Specialist* dengan pengalaman minimal 3 tahun di jabatan tersebut; atau
g. Copy Surat Keterangan Kerja sebagai *Cybersecurity Analyst / Cybersecurity Incident Analyst* dengan pengalaman minimal 2 tahun di jabatan tersebut.

9.1.3. Pemohon mengisi formulir Asesmen Mandiri (APL 02) dan dilengkapi dengan bukti pendukung yang relevan (jika ada).

9.1.4. Peserta menyatakan setuju untuk memenuhi persyaratan sertifikasi dan memberikan setiap informasi yang diperlukan untuk penilaian.

9.1.5. LSP Telekomunikasi Digital Indonesia menelaah berkas pendaftaran untuk konfirmasi bahwa peserta sertifikasi memenuhi persyaratan yang ditetapkan dalam skema sertifikasi.

9.1.6. Pemohon yang memenuhi persyaratan dinyatakan sebagai peserta sertifikasi.

9.2. Proses Asesmen

9.2.1. Asesmen skema sertifikasi direncanakan dan disusun untuk menjamin bahwa verifikasi persyaratan skema sertifikasi telah dilakukan secara obyektif dan sistematis dengan bukti terdokumentasi untukmemastikan kompetensi.

9.2.2. LSP Telekomunikasi Digital Indonesia menugaskan Asesor Kompetensi untuk melaksanakan Asesmen.

9.2.3. Asesor melakukan verifikasi persyaratan skema menggunakan perangkat asesmen dan mengkonfirmasi bukti yang akan dibuktikan dan bukti tersebut akan dikumpulkan.

9.2.4. Asesor menjelaskan, membahas dan menyepakati rincian rencana asesmen dan proses asesmen dengan Peserta Sertifikasi.

9.2.5. Asesor melakukan pengkajian dan evaluasi kecukupan bukti dari dokumen pendukung yang disampaikan pada lampiran dokumen Asesmen Mandiri APL-02, untuk memastikan bahwa bukti tersebut mencerminkan bukti yang diperlukan.

9.2.6. Peserta yang memenuhi persyaratan bukti dan menyatakan kompeten direkomendasikan untuk mengikuti proses lanjut asesmen / uji kompetensi.

9.3. Proses Uji Kompetensi

9.3.1. Uji kompetensi dirancang untuk menilai kompetensi yang dapat dilakukan dengan menggunakan metode observasi langsung / praktek demonstrasi, pertanyaan tertulis, pertanyaan lisan, verifikasi portofolio, wawancara dan metode lainnya yang andal dan objektif, serta

berdasarkan dan konsisten dengan skema sertifikasi.

9.3.2. Uji kompetensi dilaksanakan di Tempat Uji Kompetensi (TUK) yang ditetapkan melalui verifikasi oleh LSP Telekomunikasi Digital Indonesia.

9.3.3. Bukti yang dikumpulkan melalui uji kompetensi dievaluasi untuk memastikan bahwa bukti tersebut mencerminkan bukti yang diperlukan untuk memperlihatkan kompetensi telah memenuhi aturan bukti VATM.

9.3.4. Hasil proses uji kompetensi yang telah memenuhi aturan bukti VATM direkomendasikan "Kompeten" dan yang belum memenuhi aturan bukti VATM direkomendasikan "Belum Kompeten".

9.3.5. Asesor menyampaikan rekaman hasil uji kompetensi dan rekomendasi kepada LSP Telekomunikasi Digital Indonesia.

9.4. Keputusan Sertifikasi

9.4.1. LSP Telekomunikasi Digital Indonesia menjamin bahwa informasi yang dikumpulkan selama proses uji kompetensi mencukupi untuk:
a. mengambil keputusan sertifikasi;
b. melakukan penelusuran apabila terjadi banding.

9.4.2. Keputusan sertifikasi terhadap peserta hanya dilakukan oleh tim teknis pengambilan keputusan berdasarkan rekomendasi dan informasi yang dikumpulkan oleh asesor melalui proses uji kompetensi.

9.4.3. Tim teknis LSP Telekomunikasi Digital Indonesia yang bertugas membuat keputusan sertifikasi harus memiliki pengetahuan yang cukup dan pengalaman dalam proses sertifikasi untuk menentukan apakah persyaratan sertifikasi telah dipenuhi dan ditetapkan oleh LSP Telekomunikasi Digital Indonesia.

9.4.4. Keputusan sertifikasi dilakukan melalui rapat tim teknis dengan melakukan verifikasi rekomendasi dan informasi uji kompetensi dan dibuat dalam Berita Acara.

9.4.5. Keputusan pemberian sertifikat dibuat dalam surat keputusan LSP Telekomunikasi Digital Indonesia berdasarkan berita acara rapat tim teknis.

9.4.6. LSP Telekomunikasi Digital Indonesia menerbitkan sertifikat kompetensi kepada peserta yang ditetapkankompeten dalam bentuk surat dan/atau kartu, yang ditandatangani dandisahkan oleh personil yang ditunjuk LSP Telekomunikasi Digital Indonesia dengan masa berlaku sertifikat 3 **(tiga)** tahun.

9.4.7. Sertifikat diserahkan setelah seluruh persyaratan sertifikasi dipenuhi.

9.5. Pembekuan dan Pencabutan Sertifikat

9.5.1. Pembekuan dan pencabutan sertifikat dilakukan jika pemegang sertifikat melanggar kewajiban pemegang sertifikat.

9.5.2. LSP Telekomunikasi Digital Indonesia akan melakukan pembekuan

dan pencabutan sertifikat secara langsung atau melalui tahapan peringatan terlebih dahulu.

9.5.3. LSP Telekomunikasi Digital Indonesia akan memberikan pemberitahuan tertulis kepada pemegang sertifikat berkaitan dengan keputusan LSP Telekomunikasi Digital Indonesia untuk membekukan atau pencabutan sertifikat sebelum habis masa berlakunya.

9.5.4. Pemberitahuan tersebut disampaikan kepada pemegang sertifikat selambat-lambatnya 30 (tiga puluh hari) sebelum tanggal efektif pencabutan.

9.5.5. Pemegang sertifikat dapat mengajukan keberatan secara tertulis kepada LSP Telekomunikasi Digital Indonesia atas keputusan pembekuan atau pencabutan tersebut dalam jangka waktu 7 (tujuh) hari sejak tanggal surat pemberitahuan pembekuan atau pencabutan sertifikat.

9.5.6. Apabila keberatan pemegang sertifikat tidak diterima, LSP Telekomunikasi Digital Indonesia akan mengeluarkan surat pembekuan atau pencabutan secara resmi dengan memberitahukan perihal pembekuan atau pencabutan tersebutkepada pihak pemangku kepentingan terkait.

9.6. Surveilan Pemegang Sertifikat / Pemeliharaan Sertifikat

9.6.1. Pelaksanaan surveilan oleh LSP Telekomunikasi Digital Indonesia dimaksudkan untuk memastikan terpeliharanya kompetensi kerja pemegang sertifikat kompetensi.

9.6.2. Surveilan dilakukan secara periodik minimal sekali dalam satu tahun setelah diterbitkannya sertifikat kompetensi.

9.6.3. Proses surveilan dilakukan dengan metode analisis *logbook*, konfirmasi dari atasan langsung atau konfirmasi pihak ke-3, kunjungan ke tempat kerja maupun metode lain yang memungkinkan untuk memastikan keterpeliharaan kompetensi pemegang sertifikat kompetensi.

9.6.4. Hasil surveilan dicatat dalam *data base* pemegang sertifikat di LSP Telekomunikasi Digital Indonesia.

9.7. Proses Sertifikasi Ulang

9.7.1. Pemegang sertifikat wajib mengajukan permohonan sertifikasi ulang untuk memperpanjang masa berlaku sertifikat kompetensi dilakukan minimal 2 bulan sebelum masa berlaku sertifikat berakhir.

9.7.2. Proses Pendaftaran sertifikasi ulang dilakukan sesuai dengan klausul 9.1.

9.7.3. Proses asesmen / uji kompetensi sertifikasi ulang dilakukan sesuai klausul 9.2 dan 9.3.

9.7.4. Proses pengambilan keputusan sertifikasi ulang dilakukan sesuai dengan klausul 9.4.

9.8. Penggunaan Sertifikat

Pemegang sertifikat harus menandatangani persetujuan untuk :

9.8.1. Mematuhi ketentuan yang relevan dalam skema sertifikasi.

9.8.2. Menggunakan sertifikat hanya untuk ruang lingkup sertifikasi yang diberikan.

9.8.3. Tidak menggunakan sertifikat yang dapat mencemarkan / merugikan LSP Telekomunikasi Digital Indonesia dan tidak memberikan pernyataan terkait sertifikasi yang oleh LSP Telekomunikasi Digital Indonesiadianggap dapat menyesatkan atau tidak dapat dipertanggung jawabkan.

9.8.4. Menghentikan penggunaan atau pengakuan sertifikat setelah sertifikat dibekukan atau dicabut oleh LSP Telekomunikasi Digital Indonesia dan mengembalikan sertifikat kepada LSP Telekomunikasi Digital Indonesia.

9.9. Banding

9.9.1. LSP Telekomunikasi Digital Indonesia memberikan kesempatan kepada peserta untuk mengajukan banding apabila keputusan sertifikasi dirasa tidak sesuai dengan keinginannya.

9.9.2. Banding dilakukan maksimal 1 hari sejak keputusan sertifikasi ditetapkan.

9.9.3. LSP Telekomunikasi Digital Indonesia menyediakan formulir yang digunakan untuk pengajuan banding.

9.9.4. LSP Telekomunikasi Digital Indonesia membentuk tim banding yang ditugaskan untuk menangani proses banding yang beranggotakan personil yang tidak terlibat subjek yang dibanding yang dijadikan materi banding.

9.9.5. LSP Telekomunikasi Digital Indonesia menjamin bahwa proses banding dilakukan secara objektif dan tidak memihak.

9.9.6. Keputusan banding selambat-lambatnya 14 hari kerja terhitung sejak permohonan banding diterima oleh LSP Telekomunikasi Digital Indonesia.

9.9.7. Keputusan banding bersifat mengikat kedua belah pihak.