MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA

KEPUTUSAN MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA
NOMOR 120 TAHUN 2025
TENTANG
PENETAPAN STANDAR KOMPETENSI KERJA NASIONAL INDONESIA KATEGORI INFORMASI DAN KOMUNIKASI GOLONGAN POKOK AKTIVITAS PEMROGRAMAN, KONSULTASI KOMPUTER DAN KEGIATAN YANG BERHUBUNGAN DENGAN ITU (YBDI) BIDANG TANGGAP INSIDEN SIBER

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI KETENAGAKERJAAN REPUBLIK INDONESIA,

Menimbang : a. bahwa untuk melaksanakan ketentuan Pasal 31 Peraturan Menteri Ketenagakerjaan Nomor 3 Tahun 2016 tentang Tata Cara Penetapan Standar Kompetensi Kerja Nasional Indonesia, perlu menetapkan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan Yang Berhubungan Dengan Itu (YBDI) Bidang Tanggap Insiden Siber;

b. bahwa Rancangan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan Yang Berhubungan Dengan Itu (YBDI) Bidang Tanggap Insiden Siber telah disepakati melalui konvensi nasional pada tanggal 5 Desember 2024 di Jakarta;

c. bahwa sesuai surat Direktur Kebijakan Sumber Daya Manusia Keamanan Siber dan Sandi, Badan Siber dan Sandi Negara Nomor 7737/BSSN/D1/PS.02.01/12/2024 tanggal 16 Desember 2024 perihal Penyampaian Dokumen RSKKNI Bidang Tanggap Insiden Siber, perlu ditindaklanjuti dengan penetapan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan Yang Berhubungan Dengan Itu (YBDI) Bidang Tanggap Insiden Siber;

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

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. Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);
3. 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);
4. Peraturan Presiden Nomor 8 Tahun 2012 tentang Kerangka Kualifikasi Nasional Indonesia (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 24);
5. Peraturan Presiden Nomor 164 Tahun 2024 tentang Kementerian Ketenagakerjaan (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 360);
6. Peraturan Menteri Ketenagakerjaan Nomor 21 Tahun 2014 tentang Pedoman Penerapan Kerangka Kualifikasi Nasional Indonesia (Berita Negara Republik Indonesia Tahun 2014 Nomor 1792);
7. Peraturan Menteri Ketenagakerjaan Nomor 3 Tahun 2016 tentang Tata Cara Penetapan Standar Kompetensi Kerja Nasional Indonesia (Berita Negara Republik Indonesia Tahun 2016 Nomor 258);
8. Peraturan Menteri Ketenagakerjaan Nomor 20 Tahun 2024 tentang Organisasi dan Tata Kerja Kementerian Ketenagakerjaan (Berita Negara Republik Indonesia Tahun 2024 Nomor 1038);

MEMUTUSKAN:

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

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

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

KETIGA : Pemberlakuan Standar Kompetensi Kerja Nasional Indonesia sebagaimana dimaksud dalam Diktum KESATU dan penyusunan jenjang kualifikasi nasional sebagaimana dimaksud dalam Diktum KEDUA ditetapkan oleh Kepala Badan Siber dan Sandi Negara dan/atau kementerian/ lembaga teknis terkait sesuai dengan tugas dan fungsinya.

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

KELIMA : Keputusan Menteri ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 8 Mei 2025

MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA,


YASSIERLI

LAMPIRAN
KEPUTUSAN MENTERI KETENAGAKERJAAN REPUBLIK INDONESIA
NOMOR 120 TAHUN 2025
TENTANG
PENETAPAN STANDAR KOMPETENSI KERJA NASIONAL INDONESIA KATEGORI INFORMASI DAN KOMUNIKASI GOLONGAN POKOK AKTIVITAS PEMROGRAMAN, KONSULTASI KOMPUTER DAN KEGIATAN YANG BERHUBUNGAN DENGAN ITU (YBDI) BIDANG TANGGAP INSIDEN SIBER

# BAB I
# PENDAHULUAN

## A. Latar Belakang

Dalam beberapa tahun terakhir, insiden siber di Indonesia semakin meningkat baik dari segi jumlah maupun kompleksitasnya. Serangan siber yang meliputi peretasan, *malware*, *ransomware*, dan serangan *Distributed Denial of Service* (DDoS) telah menargetkan berbagai sektor, termasuk pemerintahan, keuangan, kesehatan, dan infrastruktur kritis. Data yang disajikan oleh Badan Siber dan Sandi Negara (BSSN) mengungkapkan gambaran yang mengkhawatirkan tentang lanskap ancaman siber di Indonesia. Terdapat 403.990.813 anomali yang terdeteksi sepanjang tahun 2023, termasuk 4.001.905 aktivitas *Advanced Persistent Threat* (APT) dan 1.011.209 aktivitas *ransomware*. Data ini menegaskan bahwa serangan siber bukan hanya meningkat dalam jumlah, tetapi juga dalam kompleksitas dan keparahannya. Fakta bahwa jenis trafik anomali tertinggi adalah *Generic Trojan RAT*, yang sering digunakan untuk komunikasi *backdoor* dan mengontrol server, menandakan bahwa organisasi harus meningkatkan kemampuan deteksi dan respons mereka terhadap insiden siber.

Selain itu, adanya sejumlah 1.674.185 *data exposure* pada *darknet* dan 189 kasus *web defacement* menunjukkan bahwa pelaku ancaman terus mencari celah keamanan untuk mengeksploitasi. Dengan adanya 86% aduan yang diterima berkaitan dengan *cybercrime*, urgensi untuk tindakan pencegahan dan edukasi menjadi semakin mendesak. Penanganan insiden siber di Indonesia masih menghadapi banyak tantangan. Salah satu tantangan utama adalah minimnya jumlah sumber daya manusia (SDM) yang memiliki kompetensi dalam penanganan insiden siber. Hal ini menyebabkan respon terhadap insiden sering kali tidak efektif, yang berakibat pada kerugian yang lebih besar dan pemulihan yang lebih lambat.

Berdasarkan data Pusat Perencanaan dan Pengembangan Kementerian Ketenagakerjaan, proyeksi kebutuhan tenaga kerja di sektor Teknologi Informasi dan Komunikasi (TIK) pada 2022 hingga 2025 terus meningkat. Bahkan, pada tahun 2025, diprediksi sumber daya manusia yang dibutuhkan pada sektor TIK mencapai 1.979.418 orang. Lebih detail lagi, pada kajian yang dilakukan oleh Kementerian Ketenagakerjaan setidaknya mengulas beberapa profesi yang terkait langsung dengan bidang keamanan siber. Yakni, profesi *Network Security Analyst* (proyeksi: 20.065), *Cyber Security Engineer* (proyeksi: 15.703), dan *Cryptography Researcher* (proyeksi: 1.745) dengan total proyeksi sekitar 1,4% dari total keseluruhan. Proyeksi kebutuhan Sumber Daya Manusia (SDM) di bidang

insiden respon sangat penting dalam menjawab tantangan keamanan siber yang semakin kompleks dan berkembang. Berdasarkan informasi yang ada, analisis ini akan mempertimbangkan beberapa faktor penting seperti jumlah penyedia Infrastruktur Informasi Vital (IIV) di Indonesia, ukuran dan kapabilitas organisasi, kemungkinan outsourcing, dan pembukaan sektor industri baru yang membutuhkan layanan insiden respon.

Untuk meningkatkan kapabilitas penanganan insiden siber di Indonesia, diperlukan langkah-langkah strategis yang mencakup pengembangan SDM, peningkatan koordinasi antar lembaga, dan penerapan standar yang jelas. Salah satu pendekatan yang dapat dilakukan adalah penyusunan Standar Kompetensi Kerja Nasional Indonesia (SKKNI) di bidang Tanggap Insiden Siber. SKKNI ini dapat menjadi panduan yang terstruktur untuk mengembangkan kompetensi SDM dalam menangani insiden siber secara efektif.

BSSN sebagai koordinator nasional di bidang keamanan siber memiliki peran yang sangat penting dalam upaya pengelolaan insiden siber di Indonesia. BSSN bertanggung jawab untuk memastikan koordinasi dan kolaborasi antara berbagai pemangku kepentingan, serta mengembangkan kapasitas SDM yang kompeten di bidang keamanan siber. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber memberikan kerangka kerja yang jelas untuk penanganan insiden siber di Indonesia. Peraturan ini mencakup prosedur standar untuk identifikasi, penanggulangan, dan pemulihan dari insiden siber, serta menetapkan peran dan tanggung jawab berbagai pihak yang terlibat. Dengan adanya peraturan ini, diharapkan penanganan insiden siber dapat dilakukan secara lebih terstruktur dan terkoordinasi.

Minimnya SDM yang kompeten dalam penanganan insiden siber merupakan masalah yang signifikan. Banyak organisasi yang tidak memiliki tim Tanggap Insiden Siber yang memadai, atau bahkan tidak memiliki tim khusus sama sekali. Selain itu, pendidikan dan pelatihan di bidang keamanan siber sering kali tidak mencakup seluruh aspek yang diperlukan untuk penanganan insiden secara menyeluruh. Akibatnya, ketika insiden siber terjadi, banyak organisasi yang tidak siap dan tidak mampu merespons dengan cepat dan efektif.

Penyusunan SKKNI bidang Tanggap Insiden Siber sangat penting untuk memastikan bahwa Indonesia memiliki SDM yang kompeten dan siap dalam menangani insiden siber. SKKNI ini akan menetapkan standar kompetensi yang jelas dan terukur, yang harus dimiliki oleh para profesional di bidang tanggap insiden siber. Dengan adanya SKKNI, program pelatihan dan sertifikasi dapat disesuaikan untuk memenuhi standar tersebut, sehingga menghasilkan SDM yang memiliki kemampuan dan pengetahuan yang dibutuhkan.

SKKNI bidang Tanggap Insiden Siber dirancang untuk mencapai beberapa tujuan utama, termasuk memastikan respons yang cepat dan efektif terhadap insiden siber, meminimalkan dampak yang ditimbulkan, serta mendukung pemulihan yang cepat dan menyeluruh. Dengan adanya standar kompetensi yang jelas, SDM yang terlatih akan dapat merespons insiden siber dengan cepat dan efektif, mengurangi waktu yang dibutuhkan untuk mengidentifikasi dan mengatasi ancaman. Respons yang tepat waktu akan membantu meminimalkan dampak dari insiden siber, baik dari segi kerugian finansial, kerusakan reputasi, maupun gangguan operasional. Standar kompetensi yang baik juga mencakup aspek pemulihan pasca insiden, sehingga organisasi dapat pulih dengan cepat dan kembali beroperasi secara normal.

SKKNI bidang Tanggap Insiden Siber dapat memenuhi kebutuhan kompetensi bagi individu yang akan menjadi bagian dari tim tanggap insiden siber. Standar ini mencakup berbagai keterampilan dan pengetahuan yang dibutuhkan untuk menjalankan tugas-tugas penanganan insiden siber, termasuk identifikasi dan analisis, pengelolaan respons, koordinasi dengan pihak internal dan eksternal, pemulihan sistem dan data pasca insiden siber, serta pelaporan dan dokumentasi insiden siber. Dengan adanya SKKNI bidang Tanggap Insiden Siber, diharapkan Indonesia dapat memiliki tim Tanggap Insiden Siber yang kompeten dan siap menghadapi berbagai tantangan keamanan siber di masa depan.

Jika SKKNI ini berhasil diimplementasikan dengan baik, tidak hanya akan membantu mengatasi permasalahan insiden siber, tetapi juga membuka opsi pilihan karir baru dan membuka lebih banyak lapangan pekerjaan. Dengan adanya standar kompetensi yang jelas, akan ada peningkatan permintaan untuk program pendidikan dan pelatihan yang fokus pada penanganan insiden siber, yang pada gilirannya akan menciptakan peluang karir baru di bidang keamanan siber. Selain itu, organisasi yang memiliki SDM yang kompeten akan lebih siap menghadapi ancaman siber, sehingga meningkatkan kepercayaan dan reputasi mereka di mata publik dan mitra bisnis. Dengan demikian, SKKNI bidang Tanggap Insiden Siber bukan hanya investasi dalam keamanan siber, tetapi juga dalam pembangunan ekonomi dan ketenagakerjaan di Indonesia.

B. Pengertian

1. Insiden Siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam berjalannya Sistem Elektronik.
2. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.
3. Tanggap Insiden Siber adalah serangkaian tindakan yang dilakukan untuk mengidentifikasi, melaporkan, merespons, mengatasi, dan memulihkan sistem dari Insiden Siber untuk meminimalkan dampak yang diakibatkan oleh Insiden Siber.
4. Tim Tanggap Insiden Siber adalah sekelompok orang yang bertanggung jawab menangani Insiden Siber dalam ruang lingkup yang ditentukan terhadapnya.
5. Jenis Insiden Siber adalah klasifikasi atau kategori Insiden Siber berdasarkan sifat dan karakteristik ancaman atau serangan yang terjadi.
6. Dampak Insiden Siber adalah berbagai konsekuensi atau efek negatif yang terjadi akibat serangan siber atau pelanggaran keamanan yang mempengaruhi sistem informasi, data, atau jaringan.

C. Penggunaan SKKNI

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

1. Untuk institusi pendidikan dan pelatihan
   a. Memberikan informasi untuk pengembangan program dan kurikulum.
   b. Sebagai acuan dalam penyelenggaraan pelatihan, penilaian, dan sertifikasi.
2. Untuk dunia usaha/industri dan penggunaan tenaga kerja
   a. Membantu dalam rekrutmen.
   b. Membantu penilaian unjuk kerja.

c. Membantu dalam menyusun uraian jabatan.
d. Membantu dalam mengembangkan program pelatihan yang spesifik berdasar kebutuhan dunia usaha/industri.

3. Untuk institusi penyelenggara pengujian dan sertifikasi
   a. Sebagai acuan dalam merumuskan paket-paket program sertifikasi sesuai dengan kualifikasi dan levelnya.
   b. Sebagai acuan dalam penyelenggaraan pelatihan penilaian dan sertifikasi.

D. Komite Standar Kompetensi

Susunan komite standar kompetensi pada Rancangan Standar Kompetensi Kerja Nasional Indonesia (RSKKNI) Bidang Tanggap Insiden Siber dibentuk melalui Keputusan Kepala Badan Siber dan Sandi Negara Nomor 516.4 Tahun 2024 tentang Perubahan Keputusan Kepala Badan Siber dan Sandi Negara Nomor 267 tentang Komite Penyusunan Standar Kompetensi Kerja Nasional Indonesia Bidang *Incident Response* dan Keputusan Kepala Badan Siber dan Sandi Negara Nomor 516.5 Tahun 2024 tentang Perubahan Keputusan Kepala Badan Siber dan Sandi Negara Nomor 268 tentang Pembentukan Tim Perumus, Tim Verifikasi, dan Sekretariat Penyusunan Standar Kompetensi Kerja Nasional Indonesia Bidang *Incident Response* Tahun 2024 dapat dilihat pada Tabel 1.

Tabel 1. Susunan Komite Standar Kompetensi RSKKNI Bidang Tanggap Insiden Siber

| NO. | NAMA | INSTANSI/LEMBAGA | JABATAN DALAM TIM |
|---|---|---|---|
| *1* | *2* | *3* | *4* |
| 1. | R. Tjahjo Khurniawan, S.T., M.Si. | Badan Siber dan Sandi Negara | Pengarah |
| 2. | Agus Salim, S.T., M.T. | Badan Siber dan Sandi Negara | Ketua |
| 3. | Dr. Edit Prima, M.Kom. | Badan Siber dan Sandi Negara | Sekretaris |
| 4. | Andi Yusuf, M.T. | Badan Siber dan Sandi Negara | Anggota |
| 5. | Asri Setyowati, S.Si.,M.M. | Badan Siber dan Sandi Negara | Anggota |
| 6. | Prof. Dr. Ir. Richardus Eko Indrajit, M.Sc., M.B.A., M.Phil., M.A. | ACAD-CSIRT | Anggota |
| 7. | Syarbeni, S.T. | PT Huawei Tech Investment | Anggota |

Tabel 2. Susunan Tim Perumus RSKKNI Bidang Tanggap Insiden Siber

| NO. | NAMA | INSTANSI/LEMBAGA | JABATAN DALAM TIM |
|---|---|---|---|
| *1* | *2* | *3* | *4* |
| 1. | Digit Oktavianto | Cyber Defense Community | Ketua |

| NO. | NAMA | INSTANSI/LEMBAGA | JABATAN DALAM TIM |
|---|---|---|---|
| 2. | Dr. Lucia Sri Istiyowati, S.Kom., M.Kom. | Perbanas Institute | Sekretaris |
| 3. | Satriyo Wibowo, S.T., MBA, M.H., IPM. | Indonesia Cyber Security Forum | Anggota |
| 4. | Thata Apriatin., S.Kom., M.Kom. | Indosat | Anggota |
| 5. | Rahmat Nurfauzi | PT Pijar Edukasi Teknologi (Xynexis International) | Anggota |
| 6. | Dr. Ir. Charles Lim, BSc., MSc. | ACAD-CSIRT | Anggota |
| 7. | Dr. Pratama Persadha | Communication & Information System Security Research Center (CISSRC) | Anggota |
| 8. | Iqbal Firmansyah, M.T. | PT Huawei Tech Investment | Anggota |
| 9. | Ir. Wahyu Catur Wibowo, M.Sc., Ph.D. | Universitas Indonesia | Anggota |
| 10. | Novian Nur Cahya, S.ST, M.Kom. | Badan Siber dan Sandi Negara | Anggota |
| 11. | Zegar Pradipta Putra, S.Tr.TP. | Badan Siber dan Sandi Negara | Anggota |

Tabel 3. Susunan Tim verifikasi RSKKNI Bidang Tanggap Insiden Siber

| NO. | NAMA | INSTANSI/LEMBAGA | JABATAN DALAM TIM |
|---|---|---|---|
| *1* | *2* | *3* | *4* |
| 1. | Irmawanti, S.E. | Badan Siber dan Sandi Negara | Ketua |
| 2. | Rian Irawan | Badan Siber dan Sandi Negara | Anggota |
| 3. | Galylia Aryanita Darmawan, S.ST. | Badan Siber dan Sandi Negara | Anggota |
| 4. | Dwi Destrya Sofiana, S.ST., M.M. | Badan Siber dan Sandi Negara | Anggota |
| 5. | Muhammmad Luthfi, S.Tr.Kom | Badan Siber dan Sandi Negara | Anggota |

BAB II
STANDAR KOMPETENSI KERJA NASIONAL INDONESIA

A. Pemetaan Standar Kompetensi

| TUJUAN UTAMA | FUNGSI KUNCI | FUNGSI UTAMA | FUNGSI DASAR |
|---|---|---|---|
| Melaksanakan manajemen Insiden Siber secara efektif, terstruktur, dan komprehensif guna meminimalisir Dampak Insiden Siber terhadap operasional dan aset organisasi | Melakukan pelaksanaan kesiapan terhadap Insiden Siber | Menyusun strategi komprehensif untuk penanganan Insiden Siber | Menyusun prosedur penanganan Insiden Siber |
| | | | Menguji prosedur penanganan Insiden Siber |
| | | Mempersiapkan Tim Tanggap Insiden Siber | Mengelola Tim Tanggap Insiden Siber |
| | | | Melaksanakan simulasi penanganan Insiden Siber |
| | | Mempersiapkan perangkat Tanggap Insiden Siber | Menyediakan perangkat Tanggap Insiden Siber |
| | | | Melakukan pemeliharaan perangkat Tanggap Insiden Siber |
| | Melakukan penanganan Insiden Siber | Melakukan inisiasi penanganan Insiden Siber | Melakukan konfirmasi kemungkinan terjadinya Insiden Siber |
| | | | Melakukan penilaian Dampak Insiden Siber |
| | | Melakukan penyelesaian Insiden Siber | Menganalisis insiden untuk menentukan penyebab Insiden Siber |
| | | | Melakukan penahanan terhadap Insiden Siber agar tidak berdampak lebih luas |
| | | | Menghilangkan penyebab Insiden Siber |

| TUJUAN UTAMA | FUNGSI KUNCI | FUNGSI UTAMA | FUNGSI DASAR |
|---|---|---|---|
| | | | Melakukan pemulihan sistem |
| | | | Melakukan Pelaporan Penanganan Insiden Siber |

B. Daftar Unit Kompetensi

| NO. | KODE UNIT | JUDUL UNIT KOMPETENSI |
|---|---|---|
| *1* | *2* | *3* |
| 1. | J.62TIS00.001.1 | Menyusun Prosedur Penanganan Insiden Siber |
| 2. | J.62TIS00.002.1 | Menguji Prosedur Penanganan Insiden Siber |
| 3. | J.62TIS00.003.1 | Mengelola Tim Tanggap Insiden Siber |
| 4. | J.62TIS00.004.1 | Melaksanakan Simulasi Penanganan Insiden Siber |
| 5. | J.62TIS00.005.1 | Menyediakan Perangkat Tanggap Insiden Siber |
| 6. | J.62TIS00.006.1 | Melakukan Pemeliharaan Perangkat Tanggap Insiden Siber |
| 7. | J.62TIS00.007.1 | Melakukan Konfirmasi Kemungkinan Terjadinya Insiden Siber |
| 8. | J.62TIS00.008.1 | Melakukan Penilaian Dampak Insiden Siber |
| 9. | J.62TIS00.009.1 | Menganalisis Insiden untuk Menentukan Penyebab Insiden Siber |
| 10 | J.62TIS00.010.1 | Melakukan Penahanan Terhadap Insiden Siber Agar Tidak Berdampak Lebih Luas |
| 11. | J.62TIS00.011.1 | Menghilangkan Penyebab Insiden Siber |
| 12. | J.62TIS00.012.1 | Melakukan Pemulihan Sistem |
| 13. | J.62TIS00.013.1 | Melakukan Pelaporan Penanganan Insiden Siber |

C. Uraian Unit Kompetensi

**KODE UNIT : J.62TIS00.001.1**
**JUDUL UNIT : Menyusun Prosedur Penanganan Insiden Siber**
**DESKRIPSI UNIT :** Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengidentifikasi dan membuat prosedur penanganan Insiden Siber.

| ELEMEN KOMPETENSI | KRITERIA UNJUK KERJA |
|---|---|
| 1. Menyiapkan kebutuhan penyusunan prosedur penanganan Insiden Siber | 1.1 Daftar **aset teknologi informasi** diinventarisir berdasarkan kondisi organisasi.<br>1.2 **Jenis Insiden Siber** yang ditangani ditentukan sesuai dengan daftar aset teknologi informasi. |
| 2. Membuat prosedur penanganan Insiden Siber | 2.1 **Ruang lingkup prosedur** penanganan Insiden Siber diidentifikasi berdasarkan kebutuhan organisasi.<br>2.2 Prosedur penanganan Insiden Siber disusun berdasarkan kebutuhan organisasi. |

**BATASAN VARIABEL**

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk penyiapan kebutuhan penyusunan dan pembuatan prosedur penanganan Insiden Siber.
   1.2 Aset teknologi informasi meliputi informasi, perangkat keras, perangkat lunak, dan sumber daya manusia yang bernilai dan bermanfaat untuk mencapai tujuan perusahaan/organisasi. Aset perangkat keras dapat mencakup *workstation* dan komponennya, perangkat jaringan, *printer*, *smartphone*, dan lain-lain. Aset perangkat lunak dapat mencakup lisensi, instalasi, *Operating System* (OS), dan lain-lain.
   1.3 Jenis Insiden Siber meliputi namun tidak terbatas pada kegagalan Pelindungan Data Pribadi (PDP), *malware*, serangan *phishing*, *Distributed Denial of Service* (DDoS), akses tidak sah, pencurian data, dan bentuk serangan lainnya. Masing-masing insiden memiliki karakteristik unik yang membutuhkan pendekatan dan metode penanganan yang berbeda sesuai dengan dampak dan risikonya.
   1.4 Ruang lingkup prosedur terdiri dari dan tidak terbatas pada tahapan penanganan insiden, daftar kontak pihak internal dan eksternal yang dapat dihubungi, sumber daya yang terlibat, tingkat keparahan insiden (*severity of ioncident*), waktu respon insiden, daftar proses pemulihan jaringan dan data yang penting atau kritikal, dokumen formal yang berisi langkah-langkah prosedur pemulihan, prosedur notifikasi kegagalan Pelindungan Data Pribadi (PDP), komunikasi, dan pelaporan. Prosedur dapat berupa dokumen, peraturan, pedoman, petunjuk pelaksanaan, petunjuk teknis/*guideline*/*playbook*/*runbook* atau dokumen lain yang sejenis.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat pengolah data
      2.1.2 Server/peladen yang terhubung ke jaringan

2.1.3 Perangkat lunak keamanan
2.1.4 Perangkat pemantauan jaringan
2.1.5 Sistem cadangan dan pemulihan data
2.1.6 Alat uji penetrasi dan analisis kerentanan
2.1.7 Dokumentasi prosedur keamanan siber

2.2 Perlengkapan
2.2.1 Daftar kontak pihak internal dan eksternal
2.2.2 Alat komunikasi
2.2.3 Media penyimpanan
2.2.4 *Printer*
2.2.5 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
3.1 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi
3.2 Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber
3.3 Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber
3.4 Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber

4. Norma dan standar
4.1 Norma
(Tidak ada.)
4.2 Standar
4.2.1 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27001 Keamanan Informasi, Keamanan Siber, dan Proteksi Privasi – Sistem Manajemen Keamanan Informasi – Persyaratan
4.2.2 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27035 Teknologi Informasi – Teknik Keamanan – Manajemen Insiden Keamanan Informasi
4.2.3 *National Institute of Standards and Technology Special Publication* (NIST SP) 800-61, *Rev.* 2 *Computer Security Incident Handling Guide*

**PANDUAN PENILAIAN**

1. Konteks penilaian
1.1 Penilaian/asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja atau pada tempat yang disimulasikan serta dapat diterapkan secara individu maupun sebagai bagian dari suatu kelompok.
1.2 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK).
1.3 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.
1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi,

verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Standar pengujian keamanan siber
      3.1.2 Manajemen aset teknologi informasi
      3.1.3 Manajemen risiko teknologi informasi
      3.1.4 Pengelolaan Insiden Siber
      3.1.5 Penyusunan Norma, Standar, Prosedur, dan Kriteria (NSPK)
   3.2 Keterampilan
      3.2.1 Menggunakan aplikasi pengolah kata
      3.2.2 Mengolah grafik presentasi
      3.2.3 Merancang narasi untuk dapat membuat penjelasan yang mudah dipahami mengenai prosedur penanganan Insiden Siber

4. Sikap kerja yang diperlukan
   4.1 Teliti dalam mengidentifikasi aset teknologi informasi yang berkaitan dengan pengujian keamanan siber
   4.2 Sistematis dan terstruktur dalam berpikir pada saat membuat prosedur penanganan Insiden Siber
   4.3 Patuh terhadap regulasi dan kebijakan terkait keamanan siber internal, nasional, serta internasional

5. Aspek kritis
   5.1 Ketepatan dalam mengidentifikasi ruang lingkup prosedur penanganan Insiden Siber berdasarkan kebutuhan organisasi

**KODE UNIT** : **J.62TIS00.002.1**
**JUDUL UNIT** : **Menguji Prosedur Penanganan Insiden Siber**
**DESKRIPSI UNIT**: Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam merencanakan dan melaksanakan pengujian prosedur serta proses penanganan Insiden Siber melalui pemeranan pengambilan keputusan (*tabletop exercise*).

| ELEMEN KOMPETENSI | KRITERIA UNJUK KERJA |
|---|---|
| 1. Melakukan persiapan pengujian prosedur penanganan Insiden Siber | 1.1 Rencana pengujian prosedur penanganan Insiden Siber disusun berdasarkan kebutuhan organisasi.<br>1.2 **Skenario pengujian prosedur** penanganan Insiden Siber dirancang sebagai acuan **simulasi**.<br>1.3 Pembagian peran dalam simulasi ditentukan sesuai skenario pengujian. |
| 2. Melaksanakan pengujian prosedur penanganan Insiden Siber | 2.1 Prosedur penanganan Insiden Siber disimulasikan berdasarkan skenario pengujian.<br>2.2 Hasil simulasi terhadap prosedur penanganan Insiden Siber dianalisis berdasarkan pengujian yang dilakukan.<br>2.3 Rekomendasi perbaikan prosedur penanganan Insiden Siber disusun berdasarkan hasil analisis pengujian. |

**BATASAN VARIABEL**

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk persiapan dan pelaksanaan pengujian prosedur penanganan Insiden Siber.
   1.2 Skenario pengujian prosedur merupakan sebuah proses di mana organisasi atau tim keamanan menjalankan simulasi atau tes terhadap prosedur penanganan Insiden Siber untuk memastikan bahwa semua langkah dan respon yang ada efektif dalam menghadapi serangan atau insiden keamanan nyata.
   1.3 Simulasi merupakan rangkaian proses meniru atau mereplikasi suatu situasi atau peristiwa nyata dalam kondisi yang terkendali untuk tujuan pembelajaran, pelatihan, pengujian, atau evaluasi. Dalam konteks keamanan siber atau tanggap Insiden Siber, simulasi digunakan untuk menciptakan skenario Insiden Siber sehingga prosedur penanganan Insiden Siber dapat diuji kesiapan dan kemampuannya dalam merespons insiden tanpa mengakibatkan risiko nyata pada operasi atau data.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat pengolah data
      2.1.2 Server/peladen yang terhubung ke jaringan
      2.1.3 Perangkat lunak keamanan
      2.1.4 Alat uji penetrasi dan analisis kerentanan
      2.1.5 Dokumentasi prosedur keamanan siber

2.2 Perlengkapan
2.2.1 Daftar kontak pihak internal dan eksternal
2.2.2 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
3.1 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi
3.2 Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber
3.3 Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber
3.4 Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber

4. Norma dan standar
4.1 Norma
(Tidak ada.)
4.2 Standar
4.2.1 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27001 Keamanan Informasi, Keamanan Siber, Dan Proteksi Privasi – Sistem Manajemen Keamanan Informasi – Persyaratan
4.2.2 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27035 Teknologi Informasi – Teknik Keamanan – Manajemen Insiden Keamanan Informasi
4.2.3 *National Institute of Standards and Technology Special Publication* (NIST SP) 800-61, *Rev.* 2 *Computer Security Incident Handling Guide*

**PANDUAN PENILAIAN**

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

2. Persyaratan kompetensi
(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Standar pengujian keamanan siber
      3.1.2 Manajemen aset teknologi informasi
      3.1.3 Manajemen risiko teknologi informasi
      3.1.4 Pengelolaan Insiden Siber
      3.1.5 Penyusunan Norma, Standar, Prosedur, dan Kriteria (NSPK)
   3.2 Keterampilan
      3.2.1 Menggunakan aplikasi pengolah kata
      3.2.2 Mengolah grafik presentasi
      3.2.3 Merancang narasi untuk dapat membuat penjelasan yang mudah dipahami mengenai prosedur penanganan Insiden Siber

4. Sikap kerja yang diperlukan
   4.1 Teliti dalam mengidentifikasi aset teknologi informasi yang berkaitan dengan penanganan Insiden Siber
   4.2 Sistematis dan terstruktur dalam berpikir pada saat membuat prosedur penanganan Insiden Siber

5. Aspek kritis
   5.1 Ketepatan dalam mengidentifikasi aset teknologi informasi sebagai objek pengujian sesuai dengan ruang lingkup tanggap Insiden Siber
   5.2 Ketepatan dalam merancang skenario pengujian prosedur penanganan Insiden Siber sebagai acuan simulasi

**KODE UNIT** : **J.62TIS00.003.1**
**JUDUL UNIT** : **Mengelola Tim Tanggap Insiden Siber**
**DESKRIPSI UNIT**: Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mempersiapkan pembentukan serta pengelolaan Tim Tanggap Insiden Siber.

| ELEMEN KOMPETENSI | KRITERIA UNJUK KERJA |
|---|---|
| 1. Mempersiapkan pembentukan Tim Tanggap Insiden Siber | 1.1 Peran anggota Tim Tanggap Insiden Siber dirancang sesuai dengan kebutuhan organisasi.<br>1.2 **Persyaratan pendaftaran** Tim Tanggap Insiden Siber disusun berdasarkan peraturan yang berlaku.<br>1.3 Tim Tanggap Insiden Siber didaftarkan sesuai persyaratan pendaftaran. |
| 2. Menyediakan layanan Tim Tanggap Insiden Siber | 2.1 **Layanan Tim Tanggap Insiden Siber** ditentukan sesuai dengan standar yang dipilih.<br>2.2 Komunikasi antar Tim Tanggap Insiden Siber diatur sesuai dengan protokol komunikasi yang berlaku. |

**BATASAN VARIABEL**

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk proses persiapan pembentukan dan penentuan layanan Tim Tanggap Insiden Siber.
   1.2 Persyaratan pendaftaran di antaranya sebagai berikut:
      1.2.1 Dokumen profil tim Tanggap Insiden respon dibuat berdasarkan format *request for comments* 2350.
      1.2.2 Dokumen legal yang memuat pembentukan atau pelaksanaan tugas Tim Tanggap Insiden respon.
      1.2.3 Data aset elektronik yang dapat diakses publik milik konstituen Tim Tanggap Insiden Siber dirancang sesuai dengan kebutuhan organisasi.
      1.2.4 Kompetensi sumber daya manusia Tim Tanggap Insiden Siber diinventarisir sesuai persyaratan.
   1.3 Layanan Tim Tanggap Insiden Siber tertuang pada dokumen *request for comments* 2350, layanan yang dapat diberikan di antaranya meliputi dan tidak terbatas pada:
      1.3.1 Pemberian peringatan terkait keamanan siber.
      1.3.2 Penanganan insiden siber.
      1.3.3 Penanganan kerawanan Sistem Elektronik.
      1.3.4 Penanganan artefak digital.
      1.3.5 Pemberitahuan hasil pengamatan potensi ancaman.
      1.3.6 Pendeteksian serangan.
      1.3.7 Analisis risiko keamanan siber.
      1.3.8 Konsultasi terkait kesiapan penanganan insiden siber.
      1.3.9 Pembangunan kesadaran dan kepedulian terhadap keamanan siber.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat pengolah data
      2.1.2 Jaringan internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)
      2.2.2 Alat komunikasi
      2.2.3 Media penyimpanan
      2.2.4 *Printer*

3. Peraturan yang diperlukan
   3.1 Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital
   3.2 Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber
   3.3 Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber
   3.4 Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
      4.2.1 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27001 Keamanan Informasi, Keamanan Siber, Dan Proteksi Privasi – Sistem Manajemen Keamanan Informasi – Persyaratan
      4.2.2 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27035 Teknologi Informasi – Teknik Keamanan – Manajemen Insiden Keamanan Informasi
      4.2.3 *National Institute of Standards and Technology Special Publication* (NIST SP) 800-61, *Rev.* 2 *Computer Security Incident Handling Guide*

**PANDUAN PENILAIAN**

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

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Sistem Manajemen Keamanan Informasi (SMKI)
      3.1.2 Manajemen insiden keamanan informasi
      3.1.3 Proses bisnis organisasi sesuai fungsionalitas yang akan digunakan sebagai basis dalam menentukan kapabilitas proses tanggap Insiden Siber
      3.1.4 Tata aturan, standar, dan *best practice* yang terkait dengan *security operation and incident management*
   3.2 Keterampilan
      3.2.1 Menggunakan aplikasi pengolah data

4. Sikap kerja yang diperlukan
   4.1 Objektif dalam membuat keputusan berdasarkan fakta dan data yang ada, bukan berdasarkan emosi atau asumsi
   4.2 Teliti dalam setiap langkah yang diambil selama penanganan Insiden Siber
   4.3 Tanggung jawab dalam mengambil peran dan kewajiban dengan serius, baik dalam melaksanakan tugas maupun dalam mempertanggungjawabkan hasil kerja

5. Aspek kritis
   5.1 Ketepatan dalam menyusun persyaratan pendaftaran Tim Tanggap Insiden Siber berdasarkan peraturan yang berlaku

**KODE UNIT** : **J.62TIS00.004.1**
**JUDUL UNIT** : **Melaksanakan Simulasi Penanganan Insiden Siber**
**DESKRIPSI UNIT**: Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melaksanakan simulasi penanganan Insiden Siber (*cyber drill*) untuk menguji kapabilitas dan kesiapsiagaan Tim Tanggap Insiden Siber.

| ELEMEN KOMPETENSI | KRITERIA UNJUK KERJA |
|---|---|
| 1. Menyiapkan simulasi penanganan Insiden Siber | 1.1 **Skenario penanganan Insiden Siber** dibuat sesuai prosedur.<br>1.2 **Skrip** disusun berdasarkan skenario.<br>1.3 **Sumber daya** diidentifikasi berdasarkan skrip dan skenario.<br>1.4 **Rencana simulasi penanganan Insiden Siber** disusun secara terperinci sesuai kebutuhan. |
| 2. Menjalankan simulasi penanganan Insiden Siber | 2.1 Simulasi dilaksanakan berdasarkan skenario.<br>2.2 **Hasil simulasi** dinilai berdasarkan rencana simulasi. |
| 3. Menindaklanjuti hasil simulasi penanganan Insiden Siber | 3.1 Kebutuhan latihan tambahan diidentifikasi berdasarkan hasil simulasi.<br>3.2 Rencana peningkatan kapabilitas tim Tanggap Insiden Siber disusun berdasarkan hasil identifikasi. |

**BATASAN VARIABEL**

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk merencanakan, menjalankan, dan menindaklanjuti hasil simulasi penanganan Insiden Siber.
   1.2 Skenario penanganan Insiden Siber merupakan cerita atau narasi yang menggambarkan hipotesis Insiden Siber yang akan disimulasikan. Skenario ini mencakup latar belakang, karakteristik, dan perkembangan insiden dari awal hingga akhir.
   1.3 Skrip merupakan dokumen atau rangkaian instruksi yang merinci tindakan, dialog, dan langkah-langkah yang harus diikuti oleh semua peserta selama simulasi. Skrip ini berfungsi sebagai panduan yang memastikan bahwa simulasi berjalan sesuai dengan rencana dan mencapai tujuan yang telah ditetapkan.
   1.4 Sumber daya yang dimaksud meliputi personel yang terlibat dalam simulasi serta teknologi dan sarana pendukung yang diperlukan untuk melaksanakan simulasi.
   1.5 Rencana simulasi penanganan Insiden Siber merupakan konsep pelaksanaan simulasi yang disusun secara jelas dan rinci yang mencakup sasaran atau pihak yang terlibat, dan target capaian yang diharapkan dari simulasi proses penanganan Insiden Siber.
   1.6 Hasil simulasi merupakan aspek keberhasilan dan/atau aspek kekurangan yang diidentifikasi dari pelaksanaan simulasi.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat pengolah data
      2.1.2 Perangkat lunak simulasi penanganan Insiden Siber

2.1.3 Alat komunikasi
2.2 Perlengkapan
2.2.1 Alat Tulis Kantor (ATK)
2.2.2 Media penyimpanan
2.2.3 *Printer*

3. Peraturan yang diperlukan
3.1 Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber
3.2 Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber
3.3 Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber

4. Norma dan standar
4.1 Norma
(Tidak ada.)
4.2 Standar
4.2.1 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27001 Keamanan Informasi, Keamanan Siber, Dan Proteksi Privasi – Sistem Manajemen Keamanan Informasi – Persyaratan
4.2.2 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27035 Teknologi Informasi – Teknik Keamanan – Manajemen Insiden Keamanan Informasi
4.2.3 *National Institute of Standards and Technology Special Publication* (NIST SP) 800-61, *Rev.* 2 *Computer Security Incident Handling Guide*

**PANDUAN PENILAIAN**

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

2. Persyaratan kompetensi
(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Pengelolaan Insiden Siber
      3.1.2 Sistem Manajemen Keamanan Informasi (SMKI)
   3.2 Keterampilan
      3.2.1 Mengoperasikan perangkat keras dan perangkat lunak dalam melaksanakan simulasi penanganan Insiden Siber
      3.2.2 Komunikasi efektif dalam tim

4. Sikap kerja yang diperlukan
   4.1 Proaktif dalam menindaklanjuti hasil simulasi
   4.2 Objektif dalam menyusun rencana peningkatan kapabilitas
   4.3 Kolaboratif dalam melaksanakan simulasi penanganan insiden siber

5. Aspek kritis
   5.1 Keberhasilan dalam melaksanakan simulasi penanganan Insiden Siber berdasarkan skenario penanganan Insiden Siber

**KODE UNIT** : **J.62TIS00.005.1**
**JUDUL UNIT** : **Menyediakan Perangkat Tanggap Insiden Siber**
**DESKRIPSI UNIT**: Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam proses penentuan kebutuhan dan instalasi perangkat Tanggap Insiden Siber.

| ELEMEN KOMPETENSI | KRITERIA UNJUK KERJA |
|---|---|
| 1. Menentukan kebutuhan perangkat Tanggap Insiden Siber | 1.1 **Perangkat Tanggap Insiden Siber** diidentifikasi sesuai kondisi organisasi.<br>1.2 Daftar kebutuhan perangkat Tanggap Insiden Siber disusun berdasarkan hasil identifikasi. |
| 2. Melakukan instalasi perangkat Tanggap Insiden Siber | 2.1 Perangkat Tanggap Insiden Siber dipilih sesuai **kondisi organisasi**.<br>2.2 Perangkat Tanggap Insiden Siber dikonfigurasi sesuai kebutuhan Sistem Elektronik organisasi. |

**BATASAN VARIABEL**

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk penentuan kebutuhan dan instalasi serta konfigurasi perangkat Tanggap Insiden Siber.
   1.2 Perangkat Tanggap Insiden Siber dapat berupa perangkat keras, perangkat lunak, hak penggunaan (akun, lisensi, akses), serta hal lain yang dibutuhkan dalam Tanggap Insiden Siber.
   1.3 Kondisi organisasi meliputi namun tidak terbatas pada jenis organisasi, skala organisasi, sektor organisasi, kategori Sistem Elektronik (strategis, tinggi, atau rendah), dan kondisi finansial organisasi.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat pengolah data
      2.1.2 Perangkat tanggap insiden siber
      2.1.3 Perangkat lunak pengolah kata
      2.1.4 Alat komunikasi
   2.2 Perlengkapan
      2.2.1 Dokumentasi prosedur keamanan siber
      2.2.2 Alat Tulis Kantor (ATK)
      2.2.3 Media penyimpanan
      2.2.4 *Printer*

3. Peraturan yang diperlukan
   3.1 Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber
   3.2 Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber
   3.3 Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber

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

4.2 Standar
4.2.1 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27001 Keamanan Informasi, Keamanan Siber, Dan Proteksi Privasi – Sistem Manajemen Keamanan Informasi – Persyaratan
4.2.2 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27035 Teknologi Informasi – Teknik Keamanan – Manajemen Insiden Keamanan Informasi
4.2.3 *National Institute of Standards and Technology Special Publication* (NIST SP) 800-61, *Rev.* 2 *Computer Security Incident Handling Guide*

**PANDUAN PENILAIAN**

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

2. Persyaratan kompetensi
(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
3.1 Pengetahuan
3.1.1 Perangkat Tanggap Insiden Siber
3.1.2 Proses bisnis organisasi
3.1.3 Manajemen krisis siber
3.2 Keterampilan
3.2.1 Mengoperasikan perangkat Tanggap Insiden Siber
3.2.2 Konfigurasi perangkat Tanggap Insiden Siber

4. Sikap kerja yang diperlukan
4.1 Objektif dalam menentukan kebutuhan perangkat Tanggap Insiden Siber
4.2 Teliti dalam mengkonfigurasi perangkat Tanggap Insiden Siber

5. Aspek kritis
5.1 Ketepatan dalam melakukan identifikasi perangkat Tanggap Insiden Siber sesuai dengan kondisi organisasi
5.2 Keberhasilan dalam melakukan konfigurasi perangkat Tanggap Insiden Siber sesuai dengan kebutuhan Sistem Elektronik organisasi

**KODE UNIT** : **J.62TIS00.006.1**
**JUDUL UNIT** : **Melakukan Pemeliharaan Perangkat Tanggap Insiden Siber**
**DESKRIPSI UNIT** : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melakukan persiapan pemeliharaan dan memeriksa kelayakan kondisi perangkat Tanggap Insiden Siber.

| ELEMEN KOMPETENSI | KRITERIA UNJUK KERJA |
|---|---|
| 1. Melakukan persiapan pemeliharaan perangkat Tanggap Insiden Siber | 1.1 **Prosedur pengecekan** kesesuaian kondisi perangkat Tanggap Insiden Siber ditentukan berdasarkan **praktik terbaik** *(best practice).*<br>1.2 Perangkat Tanggap Insiden Siber diinventarisir untuk memastikan ketersediaannya. |
| 2. Memeriksa kondisi perangkat Tanggap Insiden Siber | 2.1 Kondisi perangkat Tanggap Insiden Siber dilakukan tes **kelayakan**.<br>2.2 Perangkat Tanggap Insiden Siber diperbarui berdasarkan hasil tes kelayakan.<br>2.3 Dokumen hasil pemeliharaan perangkat disusun sesuai ketentuan. |

**BATASAN VARIABEL**

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk proses persiapan, pemeliharaan, pengecekan, pembaruan perangkat dan pemeriksaan kondisi perangkat Tanggap Insiden Siber.
   1.2 Prosedur pengecekan merupakan panduan yang digunakan untuk melakukan pengecekan terhadap perangkat Tanggap Insiden Siber berdasarkan regulasi yang berlaku.
   1.3 Praktik terbaik yang dimaksud merupakan cara yang paling efektif dan efisien dalam pemeriksaan kondisi perangkat Tanggap Insiden Siber.
   1.4 Kelayakan yang dimaksud merupakan kesesuaian antara kondisi aktual (hasil pengecekan) dengan kondisi normal perangkat.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat pengolah data
      2.1.2 Perangkat lunak yang digunakan untuk menguji perangkat Tanggap Insiden Siber
      2.1.3 Data spesifikasi dan petunjuk penggunaan perangkat Tanggap Insiden Siber
   2.2 Perlengkapan
      2.2.1 Dokumentasi prosedur Tanggap Insiden Siber
      2.2.2 Alat Tulis Kantor (ATK)
      2.2.3 Media penyimpanan
      2.2.4 *Printer*

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
   3.3 Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber
   3.4 Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber
   3.5 Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
      4.2.1 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27001 Keamanan Informasi, Keamanan Siber, Dan Proteksi Privasi – Sistem Manajemen Keamanan Informasi – Persyaratan
      4.2.2 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27035 Teknologi Informasi – Teknik Keamanan – Manajemen Insiden Keamanan Informasi
      4.2.3 *National Institute of Standards and Technology Special Publication* (NIST SP) 800-61, *Rev.* 2 *Computer Security Incident Handling Guide*

**PANDUAN PENILAIAN**

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

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Infrastruktur teknologi informasi

3.1.2 Perangkat jaringan
3.1.3 Manajemen insiden keamanan informasi
3.1.4 Sistem Manajemen Keamanan Informasi (SMKI)

3.2 Keterampilan
3.2.1 Mengoperasikan perangkat Tanggap Insiden Siber
3.2.2 Menyelesaikan permasalahan dalam perangkat penanganan keamanan Insiden Siber

4. Sikap kerja yang diperlukan
4.1 Teliti dalam memastikan setiap detail perangkat Tanggap Insiden Siber diperiksa secara menyeluruh
4.2 Objektif dalam menilai kondisi perangkat Tanggap Insiden Siber berdasarkan data dan hasil tes yang nyata, tanpa dipengaruhi oleh asumsi pribadi
4.3 Tanggung jawab dalam memegang komitmen untuk memelihara perangkat dengan serius dan memastikan perangkat tersebut selalu dalam kondisi siap pakai

5. Aspek kritis
5.1 Kecermatan dalam melakukan pengetesan kelayakan perangkat Tanggap Insiden Siber
5.2 Ketepatan dalam melakukan pembaruan perangkat Tanggap Insiden Siber

**KODE UNIT** : **J.62TIS00.007.1**
**JUDUL UNIT** : **Melakukan Konfirmasi Kemungkinan Terjadinya Insiden Siber**
**DESKRIPSI UNIT** : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengidentifikasi, menganalisis, memverifikasi, dan menyimpulkan potensi Insiden Siber.

| ELEMEN KOMPETENSI | KRITERIA UNJUK KERJA |
|---|---|
| 1. Mengidentifikasi kemungkinan terjadinya Insiden Siber | 1.1 **Bukti awal** insiden ditinjau menggunakan referensi silang dari berbagai sumber informasi untuk melihat adanya anomali.<br>1.2 *Alert* dari **sumber perangkat** dianalisis berdasarkan anomali yang terjadi. |
| 2. Mengumpulkan informasi yang relevan terkait kemungkinan Insiden Siber | 2.1 Bukti awal terkait Insiden Siber dari pihak pelapor didokumentasikan berdasarkan kemungkinan Insiden Siber yang terjadi.<br>2.2 Kemungkinan Insiden Siber divalidasi kepada **pemilik sistem** untuk memastikan terjadinya gangguan terhadap sistem. |
| 3. Menyiapkan materi temuan teknis terkait terjadinya Insiden Siber | 3.1 **Materi temuan teknis** disusun untuk data dukung bahan publikasi.<br>3.2 Materi temuan teknis disampaikan kepada unit terkait untuk proses publikasi. |

**BATASAN VARIABEL**

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk mengidentifikasi kemungkinan terjadinya Insiden Siber dan mengumpulkan informasi yang relevan terkait kemungkinan Insiden Siber.
   1.2 Bukti awal merupakan informasi yang diperoleh dari pelapor, dapat berupa dan tidak terbatas seperti *dashboard, log, screenshot*, atau pesan *error*. Bukti awal dapat diperoleh melalui proses komunikasi dengan pelapor untuk mendapatkan detail lebih lanjut jika diperlukan.
   1.3 Sumber perangkat terdiri dari sistem yang digunakan untuk memantau dan melaporkan aktivitas jaringan dan keamanan, meliputi namun tidak terbatas pada *Security Information and Event Management* (SIEM), perangkat keamanan jaringan, perangkat jaringan, komputer yang terhubung dengan perangkat jaringan, sistem operasi, dan aplikasi.
   1.4 Pemilik sistem merupakan entitas yang memiliki tanggung jawab atas operasi dan keamanan Sistem Elektronik. Ini mencakup organisasi yang mengoperasikan perangkat jaringan, komputer, aplikasi komputer, atau infrastruktur teknologi informasi lainnya. Pemilik sistem dapat berasal dari sektor publik atau swasta dan memiliki wewenang untuk memberikan akses atau informasi terkait untuk memastikan validasi Insiden Siber yang terjadi.
   1.5 Materi temuan teknis merupakan fakta-fakta teknis terkait terjadinya Insiden Siber yang disusun dengan bahasa yang mudah dipahami oleh publik. Ruang lingkup materi temuan teknis diantaranya namun tidak terbatas pada proses penanganan insiden yang dapat dilakukan,

langkah-langkah perbaikan terhadap pelaksanaan penanganan Insiden Siber dan dampak yang mungkin terjadi.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat pengolah data
      2.1.2 Perangkat lunak pengolah kata
   2.2 Perlengkapan
      2.2.1 Media penyimpanan
      2.2.2 *Printer*
      2.2.3 Alat komunikasi
      2.2.4 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   3.2 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
   3.3 Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber
   3.4 Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber
   3.5 Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
      4.2.1 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27001 Keamanan Informasi, Keamanan Siber, Dan Proteksi Privasi – Sistem Manajemen Keamanan Informasi – Persyaratan
      4.2.2 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27035 Teknologi Informasi – Teknik Keamanan – Manajemen Insiden Keamanan Informasi
      4.2.3 *National Institute of Standards and Technology Special Publication* (NIST SP) 800-61, *Rev.* 2 *Computer Security Incident Handling Guide*
      4.2.4 *National Institute of Standards and Technology Special Publication* (NIST SP) 800-92 *Guide to Computer Security Log Management*

**PANDUAN PENILAIAN**

1. Konteks penilaian
   1.1 Penilaian/asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja atau pada tempat yang disimulasikan serta dapat diterapkan secara individu maupun sebagai bagian dari suatu kelompok.
   1.2 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang

dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK).

1.3 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

2. Persyaratan kompetensi
(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Manajemen *log security*
      3.1.2 Jaringan komputer
      3.1.3 Proses bisnis organisasi
      3.1.4 Manajemen insiden keamanan siber
      3.1.5 Teknis yang mendalam tentang jaringan, *endpoint*, inteligensi ancaman, forensik, rekayasa balik *malware*, dan fungsi dari aplikasi spesifik atau infrastruktur teknologi informasi yang mendasarinya
   3.2 Keterampilan
      3.2.1 Mengoperasikan alat pemantauan aktivitas jaringan dan keamanan
      3.2.2 Menganalisis data berdasarkan hasil temuan pada alat pemantauan aktivitas jaringan dan keamanan
      3.2.3 Pengambilan keputusan berdasarkan data
      3.2.4 Kemampuan untuk menganalisis data dengan mendalam, mengidentifikasi pola, dan menemukan akar masalah dan bukti Insiden Siber untuk menentukan penyebab utama

4. Sikap kerja yang diperlukan
   4.1 Teliti untuk memastikan bahwa setiap bukti dan informasi dianalisis secara menyeluruh tanpa ada detail yang terlewat
   4.2 Objektif dalam membuat keputusan berdasarkan fakta dan data yang relevan, bukan berdasarkan asumsi atau emosi serta menganalisis bukti faktual dan tanpa bias

5. Aspek kritis
   5.1 Kecermatan dalam mereviu bukti awal untuk memastikan kemungkinan terjadinya Insiden Siber

**KODE UNIT** : **J.62TIS00.008.1**
**JUDUL UNIT** : **Melakukan Penilaian Dampak Insiden Siber**
**DESKRIPSI UNIT**: Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menilai Dampak Insiden Siber untuk menentukan tingkat keparahan Insiden Siber yang terjadi dalam sebuah organisasi.

| ELEMEN KOMPETENSI | KRITERIA UNJUK KERJA |
|---|---|
| 1. Melakukan identifikasi Dampak Insiden Siber pada sistem | 1.1 **Aspek keamanan informasi** diidentifikasi berdasarkan **Dampak Insiden Siber**.<br>1.2 **Jenis Insiden Siber** diklasifikasikan berdasarkan telaah indikator insiden.<br>1.3 **Tingkat keparahan Insiden Siber** dianalisis berdasarkan Dampak Insiden Siber. |
| 2. Mendokumentasikan hasil penilaian dampak | 2.2 Hasil penilaian Dampak Insiden Siber ditelaah berdasarkan tingkat keparahan.<br>2.3 Laporan hasil penilaian dampak disusun berdasarkan hasil identifikasi. |

**BATASAN VARIABEL**

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk melakukan identifikasi Dampak Insiden Siber pada sistem, menentukan penilaian Dampak Insiden Siber terhadap sistem, data, operasi bisnis, dan keamanan informasi serta mendokumentasikan hasil penilaian dampak.
   1.2 Aspek keamanan informasi meliputi integritas, kerahasiaan, dan ketersediaan data.
   1.3 Dampak Insiden Siber dapat berupa dan tidak terbatas seperti penurunan kinerja sistem, kehilangan data, kehilangan akses, gangguan layanan, dan rusaknya reputasi. Dampak Insiden Siber yang dimaksud meliputi:
      1.3.1 Dampak pada Sistem dan Data: evaluasi Dampak Insiden Siber terhadap sistem teknologi informasi dan data (kerusakan, kehilangan, atau perubahan data).
      1.3.2 Dampak pada Pelindungan Data Pribadi (PDP): merujuk pada risiko yang ditimbulkan kepada subjek data pribadi yang terdampak Insiden Siber.
      1.3.3 Dampak Operasional: nilai dampak pada operasi bisnis (*downtime*, gangguan layanan).
      1.3.4 Dampak Finansial: perkiraan kerugian finansial yang diakibatkan oleh insiden (biaya perbaikan, hilangnya pendapatan).
      1.3.5 Dampak Reputasi: pertimbangan dampak pada reputasi organisasi (kepercayaan pelanggan, kerugian *brand*).
   1.4 Jenis Insiden Siber meliputi namun tidak terbatas pada kegagalan Pelindungan Data Pribadi (PDP), *malware*, serangan *phishing*, *Distributed Denial of Service* (DDoS), akses tidak sah, pencurian data, dan bentuk serangan lainnya. Masing-masing insiden memiliki karakteristik unik yang membutuhkan pendekatan dan metode penanganan yang berbeda sesuai dengan dampak dan risikonya.
   1.5 Tingkat keparahan yang dimaksud menggunakan standar manajemen risiko organisasi. Risiko organisasi meliputi risiko operasional, risiko

finansial, risiko reputasi, risiko legal Pelindungan Data Pribadi (PDP) dalam aspek pidana, perdata, dan sanksi administrasi. Tingkat keparahan Insiden Siber dapat berupa dan tidak terbatas pada tingkatan sebagai berikut:

1.5.1 Katastropik.
1.5.2 *Critical/high.*
1.5.3 *Moderate/medium.*
1.5.4 *Low*/dapat diabaikan.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat pengolah data
      2.1.2 Perangkat lunak olah data/*log*
      2.1.3 Perangkat lunak pengolah kata
   2.2 Perlengkapan
      2.2.1 Media penyimpanan
      2.2.2 *Printer*
      2.2.3 Alat komunikasi
      2.2.4 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi
   3.2 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik
   3.3 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
   3.4 Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber
   3.5 Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber
   3.6 Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
      4.2.1 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27001 Keamanan Informasi, Keamanan Siber, Dan Proteksi Privasi – Sistem Manajemen Keamanan Informasi – Persyaratan
      4.2.2 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27035 Teknologi Informasi – Teknik Keamanan – Manajemen Insiden Keamanan Informasi
      4.2.3 Standar Nasional Indonesia - Information Technology - Security Techniques - Guidelines For Identification, Collection, Acquisition And Preservation Of Digital Evidence (SNI ISO/IEC) 27037 Teknologi Informasi - Teknik keamanan - Pedoman Identifikasi, Pengumpulan, Akuisisi Dan Preservasi Bukti Digital
      4.2.4 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI

ISO/IEC) 27701 Teknik keamanan – Ekstensi dari SNI ISO/IEC 27001 dan SNI ISO/IEC 27002 untuk Manajemen Informasi Privasi – Persyaratan Dan Pedoman

4.2.5 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 29100 Teknologi Informasi – Teknik Keamanan – Kerangka Kerja Privasi

4.2.6 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 29134 *Guidelines for Privacy Impact Assessment* Teknologi Informasi - Teknik Keamanan - Pedoman Asesmen Dampak Privasi

**PANDUAN PENILAIAN**

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

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 *Security-to-Business Integration*, pengetahuan bagaimana insiden keamanan mempengaruhi proses bisnis, pemodelan ancaman, dan penilaian serangan
      3.1.2 Sistem Manajemen Keamanan Informasi (SMKI)
      3.1.3 Jaringan komputer
      3.1.4 Proses bisnis organisasi
      3.1.5 Manajemen insiden keamanan siber
      3.1.6 Manajemen risiko
   3.2 Keterampilan
      3.2.1 Mengumpulkan dan menganalisis informasi yang diperoleh
      3.2.2 Mengoperasikan perangkat tanggap insiden siber
      3.2.3 Membuat ringkasan pengetahuan teknis

4. Sikap kerja yang diperlukan
   4.1 Teliti dalam menganalisis setiap aspek keamanan informasi dan tingkat keparahan insiden untuk memastikan hasil identifikasi Dampak Insiden Siber yang akurat

4.2 Objektif dalam penilaian Dampak Insiden Siber berdasarkan fakta dan data yang tersedia tanpa terpengaruh oleh asumsi atau pendapat subjektif
4.3 Tanggung jawab dan memiliki komitmen penuh terhadap tugas, termasuk mempertanggungjawabkan hasil penilaian dampak insiden, selalu berusaha memberikan hasil terbaik dan siap memperbaiki jika ada kesalahan

5. Aspek kritis
5.1 Ketepatan dalam menilai Dampak Insiden Siber berdasarkan pengguna dan aset terdampak yang telah diidentifikasi

**KODE UNIT** : **J.62TIS00.009.1**
**JUDUL UNIT** : **Menganalisis Insiden untuk Menentukan Penyebab Insiden Siber**
**DESKRIPSI UNIT**: Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melakukan analisis mendalam terhadap penyebab Insiden Siber (*analysis*) mencakup langkah-langkah untuk mengumpulkan informasi yang relevan, serta mengidentifikasi faktor-faktor teknis dan non-teknis yang berkontribusi terhadap Insiden Siber.

| ELEMEN KOMPETENSI | KRITERIA UNJUK KERJA |
|---|---|
| 1. Mengumpulkan informasi yang relevan tentang Insiden Siber | 1.1 **Bukti awal** yang dimiliki disusun berdasarkan urutan waktu terjadinya Insiden Siber.<br>1.2 **Spesifikasi sistem** yang terdampak Insiden Siber didokumentasikan sesuai dengan perangkat yang digunakan.<br>1.3 Pengguna pada sistem yang terdampak divalidasi berdasarkan matriks akses pengguna yang terdaftar. |
| 2. Melakukan analisis penyebab Insiden Siber | 2.1 **Faktor-faktor penyebab** terjadinya Insiden Siber dikaji berdasarkan bukti awal.<br>2.2 Penyebab Insiden Siber diuraikan lebih lanjut berdasarkan hasil kajian untuk mendapatkan hipotesis awal.<br>2.3 Hipotesis awal penyebab Insiden Siber diuji untuk mendapatkan kesimpulan penyebab insiden.<br>2.4 Kesimpulan penyebab Insiden Siber disusun sesuai dengan ketentuan. |

**BATASAN VARIABEL**

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk proses pengumpulan informasi, analisis, dan penelusuran penyebab utama dari Insiden Siber.
   1.2 Bukti awal merupakan data atau informasi yang pertama kali dikumpulkan ketika Insiden Siber terjadi atau terdeteksi. Bukti awal meliputi namun tidak terbatas pada *log* aktivitas sistem, laporan dari perangkat keamanan, pesan kesalahan, atau data lain yang menunjukkan adanya anomali atau serangan. Bukti awal dapat diperoleh melalui proses komunikasi dengan pelapor untuk mendapatkan detail lebih lanjut jika diperlukan.
   1.3 Spesifikasi sistem merujuk pada rincian teknis dari perangkat keras, perangkat lunak, dan konfigurasi jaringan yang digunakan dalam suatu sistem.
   1.4 Faktor-faktor penyebab Insiden Siber terdiri dari serangan, kegagalan tindakan organisasi dan teknikal, serta ancaman orang dalam (*insider threat*) meliputi namun tidak terbatas pada kerentanan yang terdapat dalam sistem, konfigurasi yang salah, penyusunan arsitektur yang tidak sesuai, padanan penggunaan kata sandi dan pengguna yang ada pada sistem yang tidak sesuai, kelalaian pengguna, dan kurangnya kontrol keamanan. Penyebab utama terjadinya insiden ditentukan

berdasarkan dampaknya, kemungkinan terulang, dan kompleksitas perbaikan.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat pengolah data
      2.1.2 Server/peladen yang terhubung ke jaringan
      2.1.3 Perangkat lunak pengolah kata
      2.1.4 Perangkat lunak terkait uji penetrasi
      2.1.5 Perangkat lunak keamanan
      2.1.6 Perangkat pemantauan jaringan
      2.1.7 Sistem cadangan dan pemulihan data
      2.1.8 Alat uji penetrasi dan analisis kerentanan
      2.1.9 Dokumentasi prosedur keamanan siber
   2.2 Perlengkapan
      2.2.1 Media penyimpanan
      2.2.2 *Printer*
      2.2.3 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   3.1 Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber
   3.2 Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber
   3.3 Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
      4.2.1 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27001 Keamanan informasi, keamanan siber, dan proteksi privasi – Sistem manajemen keamanan informasi – Persyaratan
      4.2.2 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27035 Teknologi informasi – Teknik Keamanan – Manajemen insiden keamanan informasi
      4.2.3 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27037 Teknologi informasi – Teknik keamanan – Pedoman identifikasi, pengumpulan, akuisisi dan preservasi bukti digital

**PANDUAN PENILAIAN**

1. Konteks penilaian
   1.1 Penilaian/asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja atau pada tempat yang disimulasikan serta dapat diterapkan secara individu maupun sebagai bagian dari suatu kelompok.
   1.2 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang

dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK).

1.3 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

2. Persyaratan kompetensi
(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Manajemen insiden keamanan informasi
      3.1.2 Sistem Manajemen Keamanan Informasi (SMKI)
      3.1.3 Layanan aset teknologi informasi yang terdampak Insiden Siber
      3.1.4 Forensik digital
   3.2 Keterampilan
      3.2.1 Mengomunikasikan proses respon terhadap Insiden Siber secara lisan dan tulisan dengan baik
      3.2.2 Mengoperasikan perangkat keras dan perangkat lunak yang mendukung proses pengambilan keputusan pengakhiran proses
      3.2.3 Mengoperasikan perangkat forensik digital

4. Sikap kerja yang diperlukan
   4.1 Cermat dalam menganalisis penyebab terjadinya Insiden Siber
   4.2 Teliti dalam memperhatikan setiap detail saat menganalisis Insiden Siber, mengumpulkan bukti, dan memastikan tidak ada informasi penting yang terlewat
   4.3 Objektif dalam memberikan penilaian hasil analisis untuk menghindari prasangka atau asumsi dalam proses analisis
   4.4 Sistematis dalam berpikir untuk memecahkan masalah kompleks menjadi bagian-bagian yang lebih sederhana untuk memudahkan analisis, serta memastikan seluruh elemen yang relevan diperhitungkan dalam menentukan akar penyebab utama Insiden Siber
   4.5 Tenang di bawah tekanan sehingga mampu bekerja secara efektif meskipun dalam situasi kritis, seperti saat Insiden Siber besar terjadi
   4.6 Berintegritas dalam memastikan hasil analisis dan tindakan yang diambil dapat dipercaya dan sesuai dengan kepentingan organisasi dan standar keamanan

5. Aspek kritis
   5.1 Kecermatan dalam menganalisis penyebab terjadinya Insiden Siber

**KODE UNIT** : **J.62TIS00.010.1**
**JUDUL UNIT** : **Melakukan Penahanan Terhadap Insiden Siber Agar Tidak Berdampak Lebih Luas**
**DESKRIPSI UNIT**: Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan untuk mengendalikan Insiden Siber dengan cara melakukan isolasi sistem yang terdampak, menerapkan pembatasan yang bersifat sementara untuk membatasi penyebaran dari Insiden Siber dengan tujuan mengurangi kerugian atau kerusakan (*containment*).

| ELEMEN KOMPETENSI | KRITERIA UNJUK KERJA |
|---|---|
| 1. Mengisolasi sistem yang terkena Insiden Siber | 1.1 Sistem yang terkena Insiden Siber dikarantina untuk mencegah eskalasi Insiden Siber.<br>1.2 Dampak karantina sistem dipetakan sesuai kategori Dampak Insiden Siber. |
| 2. Mencegah penyebaran Insiden Siber | 2.1 Semua sistem diidentifikasi keterhubungannya dengan sumber Insiden Siber.<br>2.2 **Infrastruktur cadangan** disiapkan untuk menampung sistem yang terkena Insiden Siber.<br>2.3 Sistem yang terkena Insiden Siber dipindahkan ke infrastruktur cadangan. |

**BATASAN VARIABEL**

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk mengisolasi sistem yang terkena Insiden Siber dan mencegah penyebaran Dampak Insiden Siber agar tidak meluas.
   1.2 Infrastruktur cadangan merupakan sistem atau sumber daya yang disiapkan sebagai pengganti atau dukungan terhadap infrastruktur utama jika terjadi kegagalan, gangguan, atau insiden yang mengakibatkan infrastruktur utama tidak dapat berfungsi dengan baik. Infrastruktur cadangan ini meliputi namun tidak terbatas pada segmen *network*, server, *platform* virtualisasi, aplikasi, dan data.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat pengolah data
      2.1.2 Server/peladen yang terhubung ke jaringan
      2.1.3 Perangkat lunak pengolah kata
      2.1.4 Perangkat lunak terkait uji penetrasi
      2.1.5 Perangkat lunak keamanan
      2.1.6 Perangkat pemantauan jaringan
      2.1.7 Sistem cadangan dan pemulihan data
      2.1.8 Alat uji penetrasi dan analisis kerentanan
      2.1.9 Dokumentasi prosedur keamanan siber
   2.2 Perlengkapan
      2.2.1 Media penyimpanan
      2.2.2 Media perekam
      2.2.3 *Printer*
      2.2.4 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   3.1 Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber
   3.2 Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber
   3.3 Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
      4.2.1 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27001 Keamanan informasi, keamanan siber, dan proteksi privasi – Sistem manajemen keamanan informasi – Persyaratan
      4.2.2 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27035 Teknologi informasi – Teknik Keamanan – Manajemen insiden keamanan informasi
      4.2.3 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27037 Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital

**PANDUAN PENILAIAN**

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

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Manajemen insiden keamanan informasi
      3.1.2 Sistem Manajemen Keamanan Informasi (SMKI)
      3.1.3 Sistem Operasi
      3.1.4 Pengelolaan Insiden Siber
      3.1.5 Arsitektur Jaringan dan Infrastruktur

3.2 Keterampilan
3.2.1 Mengoperasikan perangkat keras dan perangkat lunak yang mendukung proses pengendalian terhadap Insiden Siber
3.2.2 Mengoperasikan perangkat Tanggap Insiden Siber

4. Sikap kerja yang diperlukan
4.1 Tanggung jawab untuk memastikan bahwa semua langkah yang diambil dalam mengisolasi dan menangani Insiden Siber dilakukan dengan penuh kesadaran, akuntabilitas, dan sesuai dengan prosedur yang ditetapkan
4.2 Cermat dalam melakukan penahanan terhadap Insiden Siber, dengan memastikan bahwa setiap langkah yang diambil tepat sasaran dan efektif dalam mencegah penyebaran lebih lanjut
4.3 Proaktif dalam merespon potensi penyebaran Insiden Siber agar penyebaran dapat dicegah dan potensi kerusakan dapat diminimalkan sebelum berdampak lebih jauh

5. Aspek kritis
5.1 Ketepatan dalam proses karantina sistem yang terkena Insiden Siber untuk mencegah eskalasi Insiden Siber yang lebih luas

**KODE UNIT** : **J.62TIS00.011.1**
**JUDUL UNIT** : **Menghilangkan Penyebab Insiden Siber**
**DESKRIPSI UNIT**: Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam upaya penghapusan penyebab Insiden Siber serta memperkuat sistem yang terdampak Insiden Siber (*eradication*).

| ELEMEN KOMPETENSI | KRITERIA UNJUK KERJA |
|---|---|
| 1. Mengeliminasi penyebab Insiden Siber | 1.1 Penyebab Insiden Siber dinonaktifkan dari sistem.<br>1.2 Penyebab Insiden Siber dihapus sesuai kebutuhan.<br>1.3 Sistem yang terdampak **diperbarui** sesuai kebutuhan. |
| 2. Mendokumentasikan daftar penyebab Insiden Siber yang dihilangkan | 2.1 **Metode eliminasi** penyebab Insiden Siber dijabarkan berdasarkan tindakan yang dilakukan.<br>2.2 Aktivitas eliminasi penyebab Insiden Siber disusun sesuai ketentuan. |

**BATASAN VARIABEL**

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk mengeliminasi penyebab Insiden Siber serta mendokumentasikan daftar penyebab Insiden Siber yang dihilangkan.
   1.2 Diperbarui merupakan proses penutupan celah keamanan pada sistem melalui namun tidak terbatas pada perbaikan (*patching*) pada sistem yang terdampak Insiden Siber yang sudah diketahui dan dimiliki atau melakukan pembaruan konfigurasi.
   1.3 Metode eliminasi merupakan serangkaian teknik atau langkah-langkah yang digunakan untuk menghapus, menonaktifkan, atau memperbaiki penyebab utama Insiden Siber dari sistem, sehingga tidak lagi mengganggu operasi atau keamanan sistem tersebut.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat pengolah data
      2.1.2 Perangkat jaringan
      2.1.3 Perangkat lunak terkait uji penetrasi
      2.1.4 Perangkat lunak untuk mendeteksi, menonaktifkan, dan menghapus penyebab Insiden Siber
   2.2 Perlengkapan
      2.2.1 Media penyimpanan
      2.2.2 Media perekam
      2.2.3 Perangkat *patch management*
      2.2.4 *Printer*
      2.2.5 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   3.1 Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber
   3.2 Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber

3.3 Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
      4.2.1 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27001 Keamanan Informasi, Keamanan Siber, dan Proteksi Privasi – Sistem Manajemen Keamanan Informasi – Persyaratan
      4.2.2 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27035 Teknologi Informasi – Teknik Keamanan – Manajemen Insiden Keamanan Informasi
      4.2.3 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27037 Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital

**PANDUAN PENILAIAN**

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

2. Persyaratan kompetensi
   (Tidak Ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Manajemen penanganan insiden keamanan informasi
      3.1.2 Sistem Manajemen Keamanan Informasi (SMKI)
      3.1.3 Sistem Operasi
      3.1.4 Pengelolaan Insiden Siber
   3.2 Keterampilan
      3.2.1 Mengoperasikan perangkat keras dan perangkat lunak yang mendukung proses pengendalian terhadap Insiden Siber
      3.2.2 Mengoperasikan perangkat jaringan
      3.2.3 Mengoperasikan perangkat *patch management*

4. Sikap kerja yang diperlukan
   4.1 Teliti dalam mengeliminasi penyebab Insiden Siber, memastikan setiap langkah dilakukan dengan hati-hati untuk mencegah perluasan dampak
   4.2 Tanggung jawab atas setiap tindakan yang diambil selama proses eradikasi, memastikan bahwa semua langkah yang dilakukan sesuai dengan standar operasional yang berlaku
   4.3 Cermat dalam mengambil langkah yang relevan saat memperbarui sistem yang terdampak, memastikan tindakan yang diambil sesuai kebutuhan untuk mengembalikan integritas dan keamanan sistem

5. Aspek kritis
   5.1 Kecermatan dalam menghapus penyebab terjadinya Insiden Siber secara menyeluruh

**KODE UNIT** : **J.62TIS00.012.1**
**JUDUL UNIT** : **Melakukan Pemulihan Sistem**
**DESKRIPSI UNIT**: Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melakukan perbaikan dan pemulihan pada sistem yang terdampak Insiden Siber (*recovery*).

| ELEMEN KOMPETENSI | KRITERIA UNJUK KERJA |
|---|---|
| 1. Melakukan persiapan pemulihan sistem yang terkena Insiden Siber | 1.1 **Prioritas** pemulihan sistem yang terkena Insiden Siber diidentifikasi berdasarkan penilaian **Dampak Insiden Siber**.<br>1.2 **Metode pemulihan** sistem yang terkena Insiden Siber dipilih berdasarkan **hasil analisis Insiden Siber.**<br>1.3 Sumber daya perbaikan sistem yang terkena Insiden Siber ditentukan berdasarkan metode pemulihan. |
| 2. Mengembalikan sistem ke kondisi normal | 2.1 Sistem yang terkena Insiden Siber dipulihkan berdasarkan metode pemulihan yang dipilih.<br>2.2 Sistem yang telah pulih diuji sesuai dengan **skenario pengujian**.<br>2.3 Sistem yang telah lulus uji dioperasikan kembali sesuai dengan ketentuan. |
| 3. Mendokumentasikan proses pemulihan sistem | 3.1 Semua catatan perubahan sistem selama proses pemulihan sesuai dengan ketentuan.<br>3.2 Bukti sistem yang sudah pulih disimpan sesuai ketentuan. |

**BATASAN VARIABEL**

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk memulihkan sistem ke kondisi normal serta memastikan keamanan dan fungsionalitas sistem pasca insiden.
   1.2 Prioritas ditentukan berdasarkan tingkat kritikalitas aset sesuai penilaian dampak yang dapat terjadi ke organisasi.
   1.3 Dampak Insiden Siber dapat berupa dan tidak terbatas seperti penurunan kinerja sistem, kehilangan data, kehilangan akses, gangguan layanan dan rusaknya reputasi. Dampak Insiden Siber yang dimaksud meliputi:
      1.3.1 Dampak pada Sistem dan Data: evaluasi dampak insiden terhadap sistem teknologi informasi dan data (kerusakan, kehilangan, atau perubahan data).
      1.3.2 Dampak pada Pelindungan Data Pribadi (PDP): merujuk pada konsekuensi yang ditimbulkan terhadap keamanan data pribadi sebagai akibat dari Insiden Siber, seperti serangan, kebocoran data, atau akses tidak sah.
      1.3.3 Dampak Operasional: nilai dampak pada operasi bisnis (*downtime*, gangguan layanan).
      1.3.4 Dampak Finansial: perkiraan kerugian finansial yang diakibatkan oleh insiden (biaya perbaikan dan/atau hilangnya pendapatan).

1.3.5 Dampak Reputasi: pertimbangan dampak pada reputasi organisasi (kepercayaan pelanggan, kerugian *brand*).

1.4 Metode pemulihan merupakan serangkaian teknik, langkah, atau strategi yang digunakan untuk mengembalikan sistem, jaringan, atau data yang terdampak Insiden Siber kembali ke kondisi normal atau operasional. Metode pemulihan yang dimaksud secara umum meliputi namun tidak terbatas seperti: restorasi data dan sistem dari cadangan (*backup*), *patching* dan *update* sistem, rekonfigurasi sistem dan aplikasi, dan pemulihan koneksi jaringan dan komunikasi.

1.5 Hasil analisis Insiden Siber merujuk pada temuan dan kesimpulan yang diperoleh dari proses investigasi atau penyelidikan terhadap Insiden Siber yang terjadi. Analisis ini bertujuan untuk mengidentifikasi akar penyebab, jumlah aset terdampak, Dampak Insiden Siber, dan detail teknis mengenai bagaimana insiden tersebut terjadi, serta memberikan pemahaman tentang langkah-langkah yang perlu diambil untuk mitigasi dan pencegahan di masa depan. Insiden Siber yang dimaksud terdiri dari faktor-faktor penyebab terjadinya insiden dan penilaian Dampak Insiden Siber.

1.6 Skenario pengujian terdiri dari uji fungsionalitas dan uji regresi. Uji fungsionalitas yaitu proses pengujian yang dilakukan untuk memastikan bahwa sistem, perangkat lunak, atau komponen tertentu berfungsi sesuai dengan spesifikasi dan persyaratan yang telah ditentukan. Uji ini bertujuan untuk memverifikasi bahwa setiap fitur dan fungsi dari sistem berjalan dengan benar, sesuai dengan yang diharapkan, setelah mengalami perubahan, perbaikan, atau pemulihan. Sedangkan uji regresi yaitu proses pengujian untuk menjamin bahwa sistem lain tidak terdampak oleh proses pemulihan yang dilakukan.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Perangkat pengolah data

2.1.2 Perangkat keras dan lunak untuk pemulihan sistem

2.1.3 Peralatan untuk uji fungsionalitas sistem

2.1.4 Perangkat pengelolaan Insiden Siber

2.2 Perlengkapan

2.2.1 Alat Tulis Kantor (ATK)

2.2.2 Media penyimpanan

2.2.3 *Printer*

3. Peraturan yang diperlukan

3.1 Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber

3.2 Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber

3.3 Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27001 Keamanan informasi, keamanan siber, dan

proteksi privasi – Sistem manajemen keamanan informasi – Persyaratan

4.2.2 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27035 Teknologi informasi – Teknik Keamanan – Manajemen insiden keamanan informasi

4.2.3 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27037 Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital

4.2.4 *National Institute of Standards and Technology Special Publication* (NIST SP) 800-61, *Rev.* 2 *Computer Security Incident Handling Guide*

**PANDUAN PENILAIAN**

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

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Manajemen Insiden Siber
      3.1.2 Pemulihan sistem
      3.1.3 Sistem Manajemen Keamanan Informasi (SMKI)
      3.1.4 Forensik digital
   3.2 Keterampilan
      3.2.1 Menggunakan perangkat pemulihan sistem
      3.2.2 Menggunakan perangkat uji fungsionalitas sistem
      3.2.3 Menggunakan perangkat uji regresi
      3.2.4 Menggunakan perangkat pengelolaan Insiden Siber

4. Sikap kerja yang diperlukan
   4.1 Teliti dalam mengidentifikasi prioritas pemulihan sistem yang terkena Insiden Siber
   4.2 Bertanggung jawab dalam menyimpan bukti terkait sistem yang telah dipulihkan

5. Aspek kritis
   5.1 Ketepatan dalam memulihkan sistem yang terkena Insiden Siber berdasarkan metode pemulihan yang dipilih

**KODE UNIT** : **J.62TIS00.013.1**
**JUDUL UNIT** : **Melakukan Pelaporan Penanganan Insiden Siber**
**DESKRIPSI UNIT**: Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang diperlukan untuk menyusun rekomendasi dan menyampaikan laporan dalam rangka evaluasi Tanggap Insiden Siber.

| ELEMEN KOMPETENSI | KRITERIA UNJUK KERJA |
|---|---|
| 1. Membuat rekomendasi peningkatan keamanan sistem terhadap Insiden Siber | 1.1 Efektivitas **manajemen kontrol** ditinjau berdasarkan penyebab insiden yang terjadi.<br>1.2 Rekomendasi peningkatan keamanan sistem terhadap Insiden Siber disusun sesuai dengan kebutuhan. |
| 2. Membuat rekomendasi peningkatan prosedur penanganan Insiden Siber | 2.1 Proses penanganan Insiden Siber ditinjau berdasarkan **aspek sumber daya penanganan Insiden Siber**.<br>2.2 Rekomendasi peningkatan sumber daya penanganan Insiden Siber disusun berdasarkan hasil tinjauan. |
| 3. Membuat laporan Tanggap Insiden Siber | 3.1 Laporan Tanggap Insiden Siber disusun berdasarkan **aspek terkait**.<br>3.2 Laporan Tanggap Insiden Siber disampaikan sesuai kebutuhan **pemangku kepentingan**. |

**BATASAN VARIABEL**

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk membuat rekomendasi peningkatan keamanan sistem terhadap Insiden Siber, membuat rekomendasi peningkatan prosedur penanganan Insiden Siber dan membuat laporan Tanggap Insiden Siber.
   1.2 Manajemen kontrol merupakan serangkaian proses, kebijakan, dan prosedur yang diterapkan oleh organisasi untuk mengelola, mengawasi, dan memantau aktivitas sistem, serta memastikan bahwa tujuan keamanan informasi dan operasional tercapai.
   1.3 Aspek sumber daya penanganan Insiden Siber mencakup segala sesuatu yang dibutuhkan untuk memastikan insiden dapat dideteksi, dikelola, dan dipulihkan dengan baik. Ini melibatkan kombinasi antara manusia, teknologi, infrastruktur, kebijakan, dan sumber daya keuangan.
   1.4 Aspek terkait antara lain aspek yang berhubungan dengan keamanan informasi, keamanan siber, dan Pelindungan Data Pribadi.
   1.5 Pemangku kepentingan merupakan individu, kelompok, atau organisasi yang memiliki kepentingan, keterlibatan, atau pengaruh langsung atau tidak langsung terhadap keputusan, kebijakan, atau operasional suatu organisasi.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat pengolah data
      2.1.2 Perangkat lunak pengolah kata
      2.1.3 Perangkat lunak pengolah data
      2.1.4 Perangkat jaringan

2.2 Perlengkapan
2.2.1 Media penyimpanan
2.2.2 Media Perekam
2.2.3 *Printer*
2.2.4 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
3.1 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
3.2 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi
3.3 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
3.4 Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber
3.5 Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber
3.6 Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber

4. Norma dan standar
4.1 Norma
(Tidak ada.)
4.2 Standar
4.2.1 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27001 Keamanan informasi, keamanan siber, dan proteksi privasi – Sistem manajemen keamanan informasi – Persyaratan
4.2.2 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27035 Teknologi informasi – Teknik Keamanan – Manajemen insiden keamanan informasi
4.2.3 *National Institute of Standards and Technology Special Publication* (NIST SP) 800-61, *Rev.* 2 *Computer Security Incident Handling Guide*

**PANDUAN PENILAIAN**

1. Konteks penilaian
1.1 Penilaian/asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja atau pada tempat yang disimulasikan serta dapat diterapkan secara individu maupun sebagai bagian dari suatu kelompok.
1.2 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK).
1.3 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.
1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi,

verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Manajemen penanganan Insiden Siber
      3.1.2 Format laporan Insiden Siber
      3.1.3 Manajemen risiko
      3.1.4 Manajemen keamanan informasi
      3.1.5 Regulasi terkait keamanan siber
      3.1.6 Manajemen Pelindungan Data Pribadi
   3.2 Keterampilan
      3.2.1 Menggunakan perangkat pengolah kata
      3.2.2 Menggunakan perangkat pengolah data

4. Sikap kerja yang diperlukan
   4.1 Teliti untuk memastikan bahwa setiap detail informasi yang relevan dalam Insiden Siber dikumpulkan secara menyeluruh, tanpa ada data yang terlewat
   4.2 Bertanggung jawab dalam menyusun laporan yang akurat dan transparan sehingga dapat dipertanggungjawabkan di hadapan pihak yang berkepentingan
   4.3 Patuh pada regulasi untuk memastikan bahwa setiap langkah dan laporan yang dihasilkan sesuai dengan undang-undang dan peraturan yang berlaku

5. Aspek kritis
   5.1 Kecermatan dalam menyusun laporan Tanggap Insiden Siber yang akurat dan terperinci

BAB III
PENUTUP

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

MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA,

YASSIERLI