STANDAR PELAYANAN
TIM TANGGAP INSIDEN SIBER
SEKTOR ADMINISTRASI PEMERINTAHAN (Gov-CSIRT)

DEPUTI BIDANG KEAMANAN SIBER DAN SANDI

PEMERINTAHAN DAN PEMBANGUNAN MANUSIA

BADAN SIBER DAN SANDI NEGARA

Jalan Raya Muchtar No.70, Bojongsari Lama, Bojongsari,

Kota Depok, Jawa Barat

Telp : (085) 123 123 940. E-mail : govcsirt@bssn.go.id

LEMBAR PENGESAHAN DOKUMEN

STANDAR PELAYANAN
TIM TANGGAP INSIDEN SIBER
SEKTOR ADMINISTRASI PEMERINTAHAN
(Gov-CSIRT)

DEPUTI BIDANG KEAMANAN SIBER DAN
SANDI PEMERINTAHAN DAN
PEMBANGUNAN MANUSIA
BADAN SIBER DAN SANDI NEGARA

Disetujui Oleh

Deputi Bidang Keamanan Siber dan
Sandi Pemerintahan dan Pembangunan
Manusia, BSSN

Tanggal Perubahan	Riwayat Perubahan	Revisi
September 2025	Terbitan Pertama	01
-	-	-

Tanggal Efektif	Jadwal Reviu
September 2025	September 2026

DAFTAR ISI

KATA PENGANTAR

Puji dan syukur kami panjatkan ke hadirat Tuhan Yang Maha Esa karena atas berkat limpahan Rahmat dan Karunia-Nya penyusunan dokumen Standar Pelayanan Layanan Gov-CSIRT dapat diselesaikan dengan baik sebagai upaya peningkatan kualitas, acuan, serta pedoman dalam penyelenggaraan layanan publik.

Penyusunan dokumen Standar Pelayanan ini didasarkan pada Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik, Peraturan Pemerintah Nomor 96 Tahun 2012 tentang Pelaksanaan Undang-Undang Nomor 25 tahun 2009 tentang Pelayanan Publik, Pedoman Kepala Badan Siber dan Sandi Negara Nomor Tahun 2018 tentang Tata Cara Penyusunan Standar Pelayanan Publik, dan Keputusan Kepala Badaan Siber dan Sandi Negara Nomor 722 tahun 2024 tentang Tim Tanggap Insiden Siber Sektor Administrasi Pemerintahan (Gov-CSIRT) Tahun Anggaran 2024.

Sebagaimana telah diatur dalam regulasi tersebut di atas, Penyelenggara Layanan Publik memiliki tanggung jawab dalam menjamin pelayanan publik yang berkualitas, transparan, akuntabel, dan responsif terhadap kebutuhan masyarakat yang berpedoman pada prinsip-prinsip Standar Pelayanan Publik. Standar Pelayanan yang telah disusun ini menjadi dasar penyelenggaraan layanan Uji Komunikasi Gov-CSIRT dan informasi bagi masyarakat penerima layanan publik di lingkungan Badan Siber dan Sandi Negara (BSSN).

Kami sampaikan terima kasih kepada seluruh pihak yang telah berkontribusi aktif dalam penyusunan dokumen Standar Pelayanan ini. Besar harapan Standar Pelayanan ini dapat dilaksanakan dengan sebaik-baiknya sehingga mampu meningkatkan kualitas pelayanan bagi masyarakat secara berkelanjutan.

Depok, September 2025

Badan Siber dan Sandi Negara

PENDAHULUAN

A. UMUM

Badan Siber dan Sandi Negara (BSSN) dalam Peraturan Presiden Nomor 28 tahun 2021 memiliki tugas pemerintahan di bidang keamanan siber dan sandi serta melaksanakan keamanan siber secara efektif dengan mengkoordinir seluruh unsur terkait baik untuk deteksi, pemantauan, penanggulangan, pemulihan, maupun evaluasi insiden keamanan siber. Selaras dengan pelaksanaan tugas tersebut melalui Keputusan Kepala Badan Siber dan Negara Nomor 722 tahun 2024 dibentuk Tim Tanggap Insiden Siber Sektor Administrasi Pemerintahan (Gov-CSIRT) yang berada di bawah tanggung jawab Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia. Sebagaimana tertuang pada regulasi tersebut, Gov-CSIRT melaksanakan pelayanan pada lingkup Monitoring dan Aksi, Penanganan Kerentanan, dan Pembinaan dan Publikasi bagi konstituen Gov-CSIRT selaku masyarakat penerima layanan di lingkungan BSSN.

Dalam rangka menciptakan pelayanan Tanggap Insiden Siber Gov-CSIRT yang berkualitas, akuntabel, dan efektif, dibutuhkan suatu pedoman yang memuat persyaratan administratif dan operasional kegiatan dalam pemberian pelayanan Gov-CSIRT kepada konstituen yang berada di sektornya. Pedoman sebagaimana dimaksud dituangkan dalam bentuk dokumen Standar Pelayanan layanan Gov-CSIRT.

B. MAKSUD DAN TUJUAN

Standar Pelayanan Publik ini merupakan acuan yang digunakan dalam memberikan pelayanan kepada pengguna jasa dengan tujuan untuk memberikan kepastian dan meningkatkan mutu pelayanan publik.

C. SASARAN

Tercapainya kepuasan pemohon layanan atas pelayanan BSSN melalui Standar Pelayanan Publik.

STANDAR PELAYANAN
UJI KOMUNIKASI PGP-KEY

Pelayanan Publik	Uji Komunikasi PGP-Key
Dasar Hukum Pembentukan Pelayanan Publik	1. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik; 2. Peraturan Pemerintah Nomor 96 Tahun 2012 tentang Pelaksanaan Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik; 3. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara; 4. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2023 tentang Perubahan atas Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara; 5. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 271 Tahun 2024 tentang Pelayanan Publik BSSN; 6. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber; dan 7. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 722 Tahun 2024 tentang Tim Tanggap Insiden Siber Sektor Administrasi Pemerintahan (Gov-CSIRT).
Definisi Layanan	Layanan Uji Komunikasi PGP-Key merupakan kegiatan strategis yang diselenggarakan oleh Gov-CSIRT untuk memastikan proses pertukaran data sensitif antar tim penanganan insiden berlangsung secara aman, terjaga kerahasiaannya, serta hanya dapat diakses oleh pihak yang berwenang.
Persyaratan Pelayanan Publik	1. Surat Permohonan Kegiatan Uji Komunikasi 2. OpenPGP Key Email Tim Tanggap Insiden Siber
Prosedur	1. Pemohon Layanan mengirimkan surat permohonan layanan dengan tujuan kepada Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia melalui

	email govcsirt@bssn.go.id; 2. Sekretaris Gov-CSIRT menerima email dan melakukan koordinasi awal dengan pemohon layanan; 3. Sekretaris Gov-CSIRT melakukan penugasan ke unit Pembinaan dan Publikasi; 4. Kepala Unit Pembinaan dan Publikasi menugaskan anggotanya untuk melakukan proses uji komunikasi dengan tahapan : a. Melakukan *meeting* dengan pemohon layanan; b. Mengirimkan pesan simulasi email terenkripsi dengan pemohon layanan; c. Pemohon layanan melakukan dekripsi email yang telah diterima dan membalas sesuai isi pesan yang diterima; d. Melakukan validasi email balasan dari pemohon layanan; 5. Anggota Unit Pembinaan dan Publikasi menyusun laporan hasil uji komunikasi dan mengirimkan ke pemohon layanan; 6. Pemohon layanan menerima laporan hasil uji komunikasi dan mengisi tautan survey kepuasan layanan Gov-CSIRT
Jangka Waktu Pelayanan	1 (satu) hari kerja
Biaya/Tarif	Tidak dipungut biaya
Produk	Laporan Hasil Uji Komunikasi
Sarana dan Prasarana	1. Ruang layanan 2. Standar Operasional Prosedur (SOP) 3. PC/Laptop 4. Perangkat keras/lunak pendukung 5. Koneksi jaringan yang memadai
Kompetensi Pelaksana	4. Kompetensi Umum : D-IV STSN/S1 Ilmu Komputer/ S1 Teknik Informatika 5. Kompetensi Bidang : Memiliki pengetahuan dan

	keterampilan di lingkup keamanan siber 6. Kompetensi Kemampuan : a) Memiliki kemampuan pembuatan, manajemen, dan distribusi kunci OpenPGP (*public key* & *private key*); b) Memiliki kemampuan mengoperasikan perangkat lunak email yang mendukung enkripsi (misalnya Thunderbird, Evolution, atau plugin PGP); c) Memiliki kemampuan *troubleshooting* apabila terjadi kegagalan dalam proses enkripsi, dekripsi, atau verifikasi; d) Memiliki kemampuan mendokumentasikan setiap tahapan proses uji komunikasi untuk keperluan audit atau pelaporan; 7. Kepribadian dan perilaku: a) Berpenampilan rapi, ramah, dan responsif b) Mampu bekerja berdasarkan prinsip Tanggung Jawab, Integritas, Tepercaya, Sistematis, dan Akuntabel.
Pengawas Internal	Kepala Unit Pembinaan dan Publikasi Gov-CSIRT
Penanganan Pengaduan, Saran dan Masukan	Pemohon Layanan dapat melakukan pengaduan permasalahan teknis melalui: a. Surel : govcsirt@bssn.go.id b. Telepon : 085-123-123-940
Jumlah Pelaksana	2 s.d. 3 orang
Jaminan Pelayanan	Tim Penyelenggara Layanan Gov-CSIRT memberikan jaminan bahwa proses Layanan Uji Komunikasi dilaksanakan dengan proses yang cepat, mudah dan tepat.
Evaluasi Kinerja Pelaksana	Evaluasi penerapan standar layanan ini dilakukan paling sedikit 1 (satu) kali dalam 1 (satu) tahun. Selanjutnya dilakukan perbaikan untuk menjaga dan meningkatkan kinerja pelayanan.

Jaminan Keamanan Keselamatan	1. Informasi yang diberikan dijamin keabsahannya dan dapat dipertanggungjawabkan 2. Tim penyelenggara Layanan Uji Komunikasi Gov-CSIRT yang memberikan dan menerima data serta informasi telah mendapatkan penugasan dari atasan langsung
Pengguna	Pemohon layanan adalah Tim Tanggap Insiden Siber Sektor Administrasi Pemerintahan (Gov-CSIRT).

STANDAR PELAYANAN

IMPLEMENTASI *CYBER THREAT INTELLIGENCE SHARING* (CTIS) *PLATFORM*

Pelayanan Publik	Implementasi *Cyber Threat Intelligence Sharing Platform*
Dasar Hukum Pembentukan Pelayanan Publik	1. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik; 2. Peraturan Pemerintah Nomor 96 Tahun 2012 tentang Pelaksanaan Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik; 3. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara; 4. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2023 tentang Perubahan atas Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara; 5. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 271 Tahun 2024 tentang Pelayanan Publik BSSN; 6. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber; dan 7. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 722 Tahun 2024 tentang Tim Tanggap Insiden Siber Sektor Administrasi Pemerintahan (Gov-CSIRT).
Definisi Layanan	Layanan *Cyber Threat Intelligence Sharing* merupakan platform mekanisme platform kolaboratif dalam keamanan siber untuk pertukaran informasi terkait ancaman, kerentanan, serta indikator kompromi (IoC) keamanan siber. Layanan ini bertujuan untuk meningkatkan kewaspadaan dini, mempercepat proses deteksi, serta memperkuat respons terhadap serangan siber melalui berbagi data yang terstruktur, akurat, dan relevan.

Persyaratan Pelayanan Publik	1. Surat Permohonan Layanan *Cyber Threat Intelligence Sharing* 2. Informasi Narahubung Pemohon Layanan
Prosedur	1. Pemohon Layanan mengirimkan surat permohonan layanan dengan tujuan kepada Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia untuk dikirim melalui kanal email govcsirt@bssn.go.id; 2. Sekretaris Gov-CSIRT menerima email dan melakukan koordinasi awal dengan pemohon layanan; 3. Sekretaris Gov-CSIRT melakukan penugasan ke unit Monitoring dan Aksi; 4. Kepala Unit Monitoring dan Aksi menugaskan anggota untuk melakukan implementasi *Cyber Threat Intelligence Sharing Platform* dengan tahapan : a. Menyiapkan dokumen administrasi yang diperlukan (NDA, BAST, Dokumen lain); b. Pemohon Layanan mengisi dan melengkapi dokumen yang dibutuhkan, melakukan pengesahan , dan mengirim Kembali ke Gov-CSIRT; c. Melaksanakan meeting terkait pembuatan dan serah terima akun, penjelasan singkat platform; d. Melakukan bimbingan teknis pemanfaatan dan pengelolaan *platform* kepada pemohon layanan. 5. Tim Monitoring dan Aksi menyusun laporan hasil kegiatan dan mengirimkan ke pemohon layanan; 6. Pemohon layanan mengisi tautan survey kepuasan layanan Gov-CSIRT
Jangka Waktu Pelayanan	5 (lima) hari kerja
Biaya/Tarif	Tidak dipungut biaya
Produk	Akun *CTIS Platform*

Sarana dan Prasarana	1. Ruang layanan 2. Standar Operasional Prosedur (SOP) 3. PC/Laptop 4. Perangkat keras/lunak pendukung 5. Koneksi jaringan yang memadai
Kompetensi Pelaksana	1. Kompetensi Umum : D-IV STSN/S1 Ilmu Komputer/ S1 Teknik Informatika 2. Kompetensi Bidang : Memiliki pengetahuan dan keterampilan di lingkup keamanan siber 3. Kompetensi Kemampuan : a) Memahami konsep *Cyber Threat Intelligence (CTI);* b) Memahami kebijakan, regulasi, dan etika terkait berbagi data ancaman, termasuk perlindungan data dan kerahasiaan informasi. c) Mampu mengoperasikan platform CTIS untuk mengunggah, mengunduh, dan berbagi indikator ancaman; d) Mampu melakukan analisis teknis ancaman berbasis *log*, sampel *malware, traffic* jaringan, dan indikator kompromi (IoC). e) Mampu mengkorelasikan data intelijen dari berbagai sumber untuk menghasilkan wawasan yang dapat ditindaklanjuti. f) Mampu mengelola proses integrasi CTIS dengan SIEM, IDS/IPS, *firewall*, atau *endpoint security*. g) Mampu membuat laporan ancaman yang sistematis dan mudah dipahami oleh pemangku kepentingan 4. Kepribadian dan perilaku: a) Berpenampilan rapi, ramah, dan responsif b) Mampu bekerja berdasarkan prinsip Tanggung Jawab, Integritas, Tepercaya, Sistematis, dan Akuntabel.

Pengawas Internal	Kepala Unit Monitoring dan Aksi Gov-CSIRT
Penanganan Pengaduan, Saran dan Masukan	Pemohon Layanan dapat melakukan pengaduan permasalahan teknis melalui: a. Surel : govcsirt@bssn.go.id b. Telepon : 085-123-123-940
Jumlah Pelaksana	3 s.d. 5 orang
Jaminan Pelayanan	Tim Penyelenggara Layanan Gov-CSIRT memberikan jaminan bahwa proses Layanan Penanganan Aduan Kerentanan dilaksanakan dengan prinsip Tanggung Jawab, Integritas, Tepercaya, Sistematis, dan Akuntabel
Evaluasi Kinerja Pelaksana	1. Survei layanan paling sedikit 1 (satu) kali dalam 1 (satu) tahun 2. Penyusunan laporan tahunan
Jaminan Keamanan Keselamatan	1. Informasi yang diberikan dijamin keabsahannya dan dapat dipertanggungjawabkan 2. Tim penyelenggara Layanan *Cyber Threat Intelligence Sharing* Gov-CSIRT yang memberikan dan menerima data serta informasi telah mendapatkan penugasan dari atasan langsung
Pengguna	Pengguna layanan merupakan Konstituen Tim Tanggap Insiden Siber Sektor Administrasi Pemerintahan (Gov-CSIRT).

STANDAR PELAYANAN
PENANGANAN ADUAN KERENTANAN

Pelayanan Publik	Penanganan Aduan Kerentanan

Dasar Hukum Pembentukan Pelayanan Publik	1. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik; 2. Peraturan Pemerintah Nomor 96 Tahun 2012 tentang Pelaksanaan Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik; 3. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara; 4. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2023 tentang Perubahan atas Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara; 5. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 271 Tahun 2024 tentang Pelayanan Publik BSSN; 6. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber; dan 7. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 722 Tahun 2024 tentang Tim Tanggap Insiden Siber Sektor Administrasi Pemerintahan (Gov-CSIRT).
Definisi Layanan	Layanan Penanganan Aduan Kerentanan merupakan mekanisme yang disediakan oleh Gov-CSIRT untuk memfasilitasi pelaporan potensi kelemahan atau celah keamanan pada sistem informasi. Setiap aduan yang diterima akan ditindaklanjuti melalui proses verifikasi, analisis dampak, serta penentuan langkah mitigasi yang sesuai dengan standar keamanan
Persyaratan Pelayanan Publik	1. Surat Permohonan Layanan Penanganan Aduan Kerentanan 2. Dokumen/ Berkas temuan kerentanan / PoC
Prosedur	1. Pemohon Layanan mengirimkan surat permohonan layanan dengan tujuan kepada Deputi Bidang Keamanan

	Siber dan Sandi Pemerintahan dan Pembangunan Manusia untuk dikirim melalui email govcsirt@bssn.go.id; 2. Sekretaris Gov-CSIRT menerima email dan melakukan koordinasi awal dengan pemohon layanan; 3. Sekretaris Gov-CSIRT melakukan penugasan ke unit Penanganan Kerentanan; 4. Kepala Unit Penanganan Kerentanan menugaskan anggota untuk melakukan layanan Penanganan Aduan Kerentanan dengan tahapan : a. Melaksanakan Koordinasi Awal terkait temuan kerentanan; b. Melakukan proses verifikasi, validasi dan penentuan langkah mitigasi; c. Melaksanakan asistensi dan/ atau penyampaian rekomendasi tindakan mitigasi kepada Pemohon Layanan. 5. Tim Penanganan kerentanan menyusun laporan hasil kegiatan dan mengirimkan ke pemohon layanan; 6. Pemohon layanan mengisi tautan survey kepuasan layanan Gov-CSIRT.
Jangka Waktu Pelayanan	3 (tiga) hari kerja
Biaya/Tarif	Tidak dipungut biaya
Produk	Dokumen Laporan hasil validasi dan tindak lanjut kerentanan
Sarana dan Prasarana	1. Ruang layanan 2. Standar Operasional Prosedur (SOP) 3. PC/Laptop 4. Perangkat keras/lunak pendukung 5. Koneksi jaringan yang memadai
Kompetensi Pelaksana	1. Kompetensi Umum : D-IV STSN/S1 Ilmu Komputer/ S1 Teknik Informatika

	2. Kompetensi Bidang : Memiliki pengetahuan dan keterampilan di lingkup keamanan siber 3. Kompetensi Kemampuan : a. Memiliki kemampuan Mengetahui jenis-jenis kerentanan pada sistem, aplikasi, jaringan, dan perangkat b. Memiliki kemampuan penanganan kerentanan**:** identifikasi, validasi, eskalasi, mitigasi, dan pelaporan; c. Mengetahui standar dan kerangka kerja keamanan yang berlaku; d. Mampu melakukan analisis awal terhadap laporan kerentanan untuk menilai keabsahan dan tingkat keparahan (*severity*); e. Memiliki kemampuan menggunakan *tools* pengujian keamanan untuk validasi aduan; f. Mampu membuat laporan yang sistematis dan mudah dipahami oleh pemangku kepentingan. 4. Kepribadian dan perilaku: a) Berpenampilan rapi, ramah, dan responsif b) Mampu bekerja berdasarkan prinsip Tanggung Jawab, Integritas, Tepercaya, Sistematis, dan Akuntabel.
Pengawas Internal	Kepala Unit Penanganan Kerentanan Gov-CSIRT
Penanganan Pengaduan, Saran dan Masukan	Pemohon Layanan dapat melakukan pengaduan permasalahan teknis melalui: a. Surel : govcsirt@bssn.go.id b. Telepon : 085-123-123-940
Jumlah Pelaksana	3 s.d. 5 orang
Jaminan Pelayanan	Tim Penyelenggara Layanan Gov-CSIRT memberikan jaminan bahwa proses Layanan Penanganan Aduan Kerentanan dilaksanakan dengan prinsip Tanggung Jawab, Integritas, Tepercaya, Sistematis, dan Akuntabel

Evaluasi Kinerja Pelaksana	1. Survei layanan paling sedikit 1 (satu) kali dalam 1 (satu) tahun 2. Penyusunan laporan tahunan
Jaminan Keamanan Keselamatan	1. Informasi yang diberikan dijamin keabsahannya dan dapat dipertanggungjawabkan 2. Tim penyelenggara Layanan Penanganan Aduan Kerentanan Gov-CSIRT yang memberikan dan menerima data serta informasi telah mendapatkan penugasan dari atasan langsung
Pengguna	Pengguna layanan merupakan Konstituen Tim Tanggap Insiden Siber Sektor Administrasi Pemerintahan (Gov-CSIRT.

STANDAR PELAYANAN
MONITORING KEAMANAN SIBER

Pelayanan Publik	Monitoring Keamanan Siber
Dasar Hukum Pembentukan Pelayanan Publik	1. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik; 2. Peraturan Pemerintah Nomor 96 Tahun 2012 tentang Pelaksanaan Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik; 3. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara; 4. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2023 tentang Perubahan atas Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara; 5. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 271 Tahun 2024 tentang Pelayanan Publik BSSN; 6. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber; dan 7. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 722 Tahun 2024 tentang Tim Tanggap Insiden Siber Sektor Administrasi Pemerintahan (Gov-CSIRT).
Definisi Layanan	Layanan Monitoring Keamanan Siber merupakan kegiatan yang diselenggarakan oleh Gov-CSIRT untuk melakukan monitoring keamanan siber melalui implementasi *endpoint security* pada konstituen Gov-CSIRT.
Persyaratan Pelayanan Publik	Surat Permohonan Layanan Monitoring Keamanan SIber
Prosedur	1. Pemohon Layanan mengirimkan surat permohonan layanan dengan tujuan kepada Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia untuk dikirim melalui email ke govcsirt@bssn.go.id;

	2. Sekretaris Gov-CSIRT menerima email dan melakukan koordinasi awal dengan pemohon layanan; 3. Sekretaris Gov-CSIRT melakukan penugasan ke unit Monitoring dan Aksi; 4. Kepala Unit Monitoring dan Aksi menugaskan anggota untuk melaksanakan Monitoring Keamanan Siber dengan tahapan: a. Melakukan Koordinasi terkait Layanan Monitoring bersama pemohon layanan b. Menyusun NDA/Surat Persetujuan implementasi layanan monitoring c. Melakukan konfigurasi akun user untuk pemohon layanan d. Melakukan implementasi layanan dan pengujian fungsi pada perangkat pemohon layanan e. Melakukan bimbingan teknis operasional perangkat monitoring kepada pemohon layanan 5. Tim Monitoring dan Aksi menyusun laporan hasil kegiatan dan mengirimkan ke pemohon layanan; 6. Pemohon layanan mengisi tautan survey kepuasan layanan Gov-CSIRT.
Jangka Waktu Pelayanan	5 (lima) hari kerja
Biaya/Tarif	Tidak dipungut biaya
Produk	Laporan Hasil Monitoring Keamanan Siber
Sarana dan Prasarana	1. Ruang layanan 2. Standar Operasional Prosedur (SOP) 3. PC/Laptop 4. Perangkat keras/lunak pendukung 5. Koneksi jaringan yang memadai
Kompetensi Pelaksana	1. Kompetensi Umum : D-IV STSN/S1 Ilmu Komputer/ S1 Teknik Informatika

	2. Kompetensi Bidang : Memiliki pengetahuan dan keterampilan di lingkup keamanan siber 3. Kompetensi Kemampuan : a) Memiliki kemampuan mengoperasikan sistem *Security Information and Event Management* (SIEM) dan platform monitoring lainnya; b) Mampu melakukan analisis *log*, *event*, dan *alert* untuk mendeteksi anomali atau aktivitas mencurigakan; c) Mengetahui indikator kompromi (IoC) dan teknik serangan siber yang umum digunakan; d) Mampu melakukan korelasi data dari berbagai sumber (jaringan, aplikasi, *endpoint*) untuk mengidentifikasi potensi insiden; e) Memiliki kemampuan membuat eskalasi temuan secara tepat waktu kepada tim tanggap insiden; f) Mampu menyusun laporan hasil monitoring yang sistematis, ringkas, dan mudah dipahami oleh pemangku kepentingan. 4. Kepribadian dan perilaku: a) Berpenampilan rapi, ramah, dan responsif b) Mampu bekerja berdasarkan prinsip Tanggung Jawab, Integritas, Tepercaya, Sistematis, dan Akuntabel.
Pengawas Internal	Kepala Unit Monitoring dan Aksi Gov-CSIRT
Penanganan Pengaduan, Saran dan Masukan	Pemohon Layanan dapat melakukan pengaduan permasalahan teknis melalui: a. Surel : govcsirt@bssn.go.id b. Telepon : 085-123-123-940
Jumlah Pelaksana	3 s.d. 5 orang
Jaminan Pelayanan	Tim Penyelenggara Layanan Gov-CSIRT memberikan jaminan bahwa proses Layanan Monitoring Keamanan Siber dilaksanakan dengan prinsip Tanggung Jawab, Integritas,

	Tepercaya, Sistematis, dan Akuntabel
Evaluasi Kinerja Pelaksana	1. Survei layanan paling sedikit 1 (satu) kali dalam 1 (satu) tahun 2. Penyusunan laporan tahunan
Jaminan Keamanan Keselamatan	1. Informasi yang diberikan dijamin keabsahannya dan dapat dipertanggungjawabkan 2. Tim penyelenggara Layanan Monitoring Keamanan Siber Gov-CSIRT yang memberikan dan menerima data serta informasi telah mendapatkan penugasan dari atasan langsung
Pengguna	Pengguna layanan merupakan Konstituen Tim Tanggap Insiden Siber Sektor Administrasi Pemerintahan (Gov-CSIRT).

STANDAR PELAYANAN
UJI PENETRASI

Pelayanan Publik	Uji Penetrasi
Dasar Hukum Pembentukan Pelayanan Publik	1. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik; 2. Peraturan Pemerintah Nomor 96 Tahun 2012 tentang Pelaksanaan Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik; 3. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara; 4. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2023 tentang Perubahan atas Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara; 5. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 271 Tahun 2024 tentang Pelayanan Publik BSSN; 6. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber; dan 8. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 722 Tahun 2024 tentang Tim Tanggap Insiden Siber Sektor Administrasi Pemerintahan (Gov-CSIRT).
Definisi Layanan	Layanan Uji Penetrasi merupakan kegiatan strategis yang diselenggarakan oleh Gov-CSIRT untuk membantu percepatan Tim Tanggap Insiden Siber (TTIS) Organisasi pada sektor administrasi pemerintahan dalam mengidentifikasi, mengevaluasi, dan memperbaiki kerentanan sistem sehingga meningkatkan ketahanan keamanan siber.
Persyaratan Pelayanan Publik	Surat Permohonan Layanan Uji Penetrasi
Prosedur	1. Pemohon Layanan mengirimkan surat permohonan layanan dengan tujuan kepada Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan

	Manusia untuk dikirim melalui email ke govcsirt@bssn.go.id; 2. Sekretaris Gov-CSIRT menerima email dan melakukan koordinasi awal dengan pemohon layanan; 3. Sekretaris Gov-CSIRT melakukan penugasan ke unit Monitoring dan Aksi; 4. Kepala Unit Monitoring dan Aksi menugaskan anggota untuk melakukan proses Uji Penetrasi dengan tahapan : a. Melakukan *meeting* dengan pemohon layanan untuk menentukan target, metode, jadwal, serta aturan keterlibatan (rules of engagement); b. Melakukan tahap *reconnaissance* & *scanning* terhadap sistem, aplikasi, atau jaringan yang menjadi target; c. Melaksanakan eksploitasi terhadap kerentanan yang ditemukan dengan tetap memperhatikan batasan dan etika pengujian; d. Melakukan pasca-eksploitasi untuk menilai dampak, bukti akses, serta potensi eskalasi hak istimewa; e. Mendokumentasikan seluruh temuan, bukti uji, dan langkah yang dilakukan selama pengujian; f. Pemohon layanan melakukan perbaikan hasil temuan dengan mengisi form perbaikan hasil pengujian g. Melakukan review hasil perbaikan yang dilakukan pemohon layanan 5. Tim Monitoring dan Aksi menyusun laporan hasil Uji Penetrasi dan mengirimkan ke pemohon layanan; 6. Pemohon layanan menerima laporan hasil uji komunikasi dan mengisi tautan survey kepuasan layanan Gov-CSIRT.
Jangka Waktu Pelayanan	5 (lima) hari kerja
Biaya/Tarif	Tidak dipungut biaya
Produk	Laporan Hasil Uji Penetrasi dan Rekomendasi Tindakan Mitigasi

Sarana dan Prasarana	1. Ruang layanan 2. Standar Operasional Prosedur (SOP) 3. PC/Laptop 4. Perangkat keras/lunak pendukung 5. Koneksi jaringan yang memadai
Kompetensi Pelaksana	1. Kompetensi Umum : D-IV STSN/S1 Ilmu Komputer/ S1 Teknik Informatika 2. Kompetensi Bidang : Memiliki pengetahuan dan keterampilan di lingkup keamanan siber 3. Kompetensi Kemampuan : a) Memiliki kemampuan memahami arsitektur jaringan, aplikasi, sistem operasi, dan perangkat keras; b) Mampu mengidentifikasi, mengeksploitasi, dan mendokumentasikan kerentanan pada sistem, aplikasi, jaringan, maupun perangkat; c) Mengetahui metodologi uji penetrasi yang diakui (misalnya OWASP, PTES, OSSTMM, NIST); d) Memiliki kemampuan menggunakan berbagai *tools* uji penetrasi (seperti Burp Suite, Metasploit, Nmap, Wireshark, dan sejenisnya); e) Mampu melakukan pengujian secara manual untuk menemukan kerentanan yang tidak terdeteksi oleh *tools* otomatis; f) Memiliki kemampuan menyusun laporan hasil uji penetrasi yang mencakup temuan, tingkat risiko, bukti, serta rekomendasi mitigasi; g) Mengetahui prinsip etika dan legalitas dalam pelaksanaan uji penetrasi serta menjaga kerahasiaan data.; 4. Kepribadian dan perilaku: a) Berpenampilan rapi, ramah, dan responsif b) Mampu bekerja berdasarkan prinsip Tanggung Jawab, Integritas, Tepercaya, Sistematis, dan Akuntabel.

Pengawas Internal	Kepala Unit Monitoring dan Aksi Gov-CSIRT
Penanganan Pengaduan, Saran dan Masukan	Pemohon Layanan dapat melakukan pengaduan permasalahan teknis melalui: a. Surel : govcsirt@bssn.go.id b. Telepon : 085-123-123-940
Jumlah Pelaksana	3-5 orang
Jaminan Pelayanan	Tim Penyelenggara Layanan Gov-CSIRT memberikan jaminan bahwa proses Layanan Monitoring keamanan Siber dilaksanakan dengan prinsip Tanggung Jawab, Integritas, Tepercaya, Sistematis, dan Akuntabel
Evaluasi Kinerja Pelaksana	1. Survei layanan paling sedikit 1 (satu) kali dalam 1 (satu) tahun 2. Penyusunan laporan tahunan
Jaminan Keamanan Keselamatan	1. Informasi yang diberikan dijamin keabsahannya dan dapat dipertanggungjawabkan 2. Tim penyelenggara Layanan Uji Penetrasi Keamanan Siber Gov-CSISRT yang memberikan dan menerima data serta informasi telah mendapatkan penugasan dari atasan langsung
Pengguna	Pengguna layanan merupakan Konstituen Tim Tanggap Insiden Siber Sektor Administrasi Pemerintahan (Gov-CSIRT).

STANDAR PELAYANAN
TANGGAP INSIDEN SIBER

Pelayanan Publik	Tanggap Insiden Siber
Dasar Hukum Pembentukan Pelayanan Publik	1. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik; 2. Peraturan Pemerintah Nomor 96 Tahun 2012 tentang 3. Pelaksanaan Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik; 4. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara; 5. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2023 tentang Perubahan atas Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara; 6. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 271 Tahun 2024 tentang Pelayanan Publik BSSN; 7. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber; dan 8. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 722 Tahun 2024 tentang Tim Tanggap Insiden Siber Sektor Administrasi Pemerintahan (Gov-CSIRT).
Definisi Layanan	Layanan Tanggap Insiden Siber merupakan kegiatan yang diselenggarakan oleh Gov-CSIRT untuk membantu percepatan Tim Tanggap Insiden Siber (TTIS) Organisasi pada sektor administrasi pemerintahan dalam merespons, menangani, dan memulihkan insiden siber secara efektif sehingga mengurangi dampak serta meningkatkan kesiapsiagaan dan ketahanan keamanan siber.
Persyaratan Pelayanan Publik	Surat Permohonan Layanan Tanggap Insiden Siber
Prosedur	1. Pemohon Layanan mengirimkan surat permohonan layanan dengan tujuan kepada Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan

Manusia untuk dikirim melalui email ke govcsirt@bssn.go.id;

2. Sekretaris Gov-CSIRT menerima email dan melakukan koordinasi awal dengan pemohon layanan;
3. Sekretaris Gov-CSIRT melakukan penugasan ke unit Monitoring dan Aksi;
4. Kepala Unit Monitoring dan Aksi menugaskan anggota untuk melakukan proses Uji Penetrasi dengan tahapan :
    a. Melakukan *meeting* dengan pemohon layanan untuk menentukan target, metode, jadwal, serta aturan keterlibatan (rules of engagement);
    b. Melakukan identifikasi dan verifikasi insiden melalui pengumpulan log, bukti digital, serta informasi pendukung lainnya;
    c. Melakukan analisis insiden untuk menentukan vektor serangan, jenis ancaman, serta sistem yang terdampak;
    d. Melaksanakan tindakan mitigasi awal untuk menghentikan atau membatasi penyebaran insiden sesuai dengan tingkat keparahan;
    e. Melakukan pemulihan sistem yang terdampak serta memastikan integritas dan ketersediaan layanan kembali normal;
    f. Mendokumentasikan seluruh proses penanganan insiden, termasuk kronologi, bukti teknis, serta tindakan yang telah dilakukan;
    g. Memberikan rekomendasi perbaikan dan peningkatan keamanan kepada pemohon layanan berdasarkan hasil penanganan insiden;
    h. Menutup insiden setelah konfirmasi pemulihan dan penyelesaian tindak lanjut, serta melakukan evaluasi untuk peningkatan proses di masa mendatang.
7. Tim Monitoring dan Aksi menyusun laporan hasil Tanggap Insiden Siber dan mengirimkan ke pemohon layanan;
8. Pemohon layanan menerima laporan hasil Tanggap Insiden Siber dan mengisi tautan survey kepuasan layanan Gov-CSIRT.

Jangka Waktu Pelayanan	5 (lima) hari kerja
Biaya/Tarif	Tidak dipungut biaya
Produk	Laporan Hasil Tanggap Insiden Siber
Sarana dan Prasarana	1. Ruang layanan 2. Standar Operasional Prosedur (SOP) 3. PC/Laptop 4. Perangkat keras/lunak pendukung 5. Koneksi jaringan yang memadai
Kompetensi Pelaksana	1. Kompetensi Umum : D-IV STSN/S1 Ilmu Komputer/ S1 Teknik Informatika 2. Kompetensi Bidang : Memiliki pengetahuan dan keterampilan di lingkup keamanan siber 3. Kompetensi Kemampuan : a) Memiliki kemampuan Mengetahui jenis-jenis insiden siber; b) Memiliki kemampuan penanganan insiden siber: investigas, mitigasi, dan pelaporan; c) Mengetahui standar dan kerangka kerja keamanan yang berlaku; d) Mampu melakukan analisis awal terhadap laporan aduan insiden siber; e) Memiliki kemampuan menggunakan *tools* penanganan insiden siber; f) Memiliki kemampuan menyusun laporan hasil tanggap insiden siber yang mencakup kronologi, bukti teknis, rekomendasi mitigasi, dan langkah tindak lanjut; g) Mengetahui prinsip etika, kepatuhan hukum, perlindungan data pribadi, serta prosedur pelaporan ke pihak berwenang dan pemangku kepentingan.

	4. Kepribadian dan perilaku: a) Berpenampilan rapi, ramah, dan responsif b) Mampu bekerja berdasarkan prinsip Tanggung Jawab, Integritas, Tepercaya, Sistematis, dan Akuntabel.
Pengawas Internal	Kepala Unit Monitoring dan Aksi Gov-CSIRT
Penanganan Pengaduan, Saran dan Masukan	Pemohon Layanan dapat melakukan pengaduan permasalahan teknis melalui: a. Surel : govcsirt@bssn.go.id b. Telepon : 085-123-123-940
Jumlah Pelaksana	2 s.d. 3 orang
Jaminan Pelayanan	Tim Penyelenggara Layanan Gov-CSIRT memberikan jaminan bahwa proses Layanan Tanggap Insiden Siber keamanan Siber dilaksanakan dengan prinsip Tanggung Jawab, Integritas, Tepercaya, Sistematis, dan Akuntabel
Evaluasi Kinerja Pelaksana	1. Survei layanan paling sedikit 1 (satu) kali dalam 1 (satu) tahun 2. Penyusunan laporan tahunan
Jaminan Keamanan Keselamatan	1. Informasi yang diberikan dijamin keabsahannya dan dapat dipertanggungjawabkan 2. Tim penyelenggara Layanan Uji Penetrasi Keamanan Siber Gov-CSISRT yang memberikan dan menerima data serta informasi telah mendapatkan penugasan dari atasan langsung
Pengguna	Pengguna layanan merupakan Konstituen Tim Tanggap Insiden Siber Sektor Administrasi Pemerintahan (Gov-CSIRT).