RFC 2350 CSIRT-STMIKJ

1. Informasi mengenai dokumen ini berisi deskripsi CSIRT-STMIKJ berdasarkan RFC 2350, yaitu informasi dasar mengenai CSIRT-STMIKJ, menjelaskan tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi CSIRT-STMIKJ.
   1.1. Tanggal update terakhir dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 3 Desember 2024
   1.2. Tidak ada daftar distribusi untuk pemberitahuan mengenai pembaharuan dokumen.
   1.3. Lokasi dimana dokumen ini bisa didapat versi terbaru dari dokumen ini tersediapada web https://repository.stmikjayakarta.ac.id/csirt
   1.4. Keaslian kedua dokumen (versi bahasa inggris dan bahasa Indonesia) adalahdokumen yang telah ditanda tangani Kepala CSIRT-STMIKJ.
   1.5. Identifikasi dokumen kedua dokumen (versi bahasa inggris dan bahasa Indonesia) memiliki atribut yang sama, yaitu:

1.5.2.	Judul	: RFC 2350 CSIRT-STMIKJ
1.5.3.	Versi	: 1.0
1.5.4.	Tanggal Publikasi	: 3 Desember 2024
1.5.5.	Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak
   2.1. Nama Tim Computer Security Incident Response Team Sekolah Tinggi Ilmu Manajemen Informatika dan Komputer Jayakarta disingkat dengan CSIRT-STMIKJ.
   2.2. Alamat Jl. Salemba Raya No.24, RT.4/RW.6, Kenari, Kec. Senen, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10430,Indonesia.
   2.3. Zona Waktu Jakarta (GMT+07:00)

2.4. Nomor Telepon +62 213906060

2.5. NomorFax +623905050

2.6. Nomor Helpdesk CSIRT-STMIKJ +62 8128065138

2.6. Alamat Surat Elektronik (E-mail) csirt[at]stmik.jayakarta.ac.id

2.7. Anggota Tim

Ketua CSIRT-STMIKJ adalah Ketua Program Studi S1-Teknik Informatika dengan anggota tim perwakilan dari Dosen STMIK Jayakarta.

2.8. Informasi/data lain Tidak ada.

2.9. Catatan-catatan pada Kontak CSIRT-STMIKJ

Metode yang disarankan untuk menghubungi CSIRT-STMIKJ adalah melalui e-mail pada alamat csirt[at]stmikjayakarta.ac.id atau melalui nomor telepon (+628128065138) ke CSIRT-STMIKJ yang siaga selama 24/7.

3. Mengenai CSIRT-STMIKJ

3.1. Visi CSIRT-STMIKJ adalah terwujudnya ketahanan siber pada sektor pendidikan yang handal dan profesional di lingkungan STMIK Jayakarta.

3.2. Misi dari CSIRT-STMIKJ, yaitu:

3.2.1. Mengoordinasikan dan mengolaborasikan layanan keamanan siber pada kampus baik internal dan eksternal di lingkungan STMIK Jayakarta.

3.2.2. Mengidentifikasi kerentanan keamanan secara menyeluruh

3.2.3. Meningkatkan respons aspek keamanan kepada seluruh Satuan Unit Kerja di kampus STMIK Jayakarta.

3.2.4. Meningkatkan mutu layanan TIK Pendidikan, Kebudayaan, Riset danTeknologi dari ancaman siber.

3.3. Konstituen

Konstituen CSIRT-STMIKJ adalah seluruh satuan unit kerja kampus STMIK Jayakarta.

3.4. Sponsorship dan/atau Afiliasi

Sponsorship dan/atau Afiliasi CSIRT-STMIKJ merupakan bagian dari akademik sehingga seluruh pembiayaan bersumber dari kampus.

4. Kebijakan–Kebijakan

4.1. Jenis-jenis insiden dan tingkat/level Dukungan CSIRT-STMIKJ memiliki otoritasuntuk menangani insiden yaitu:

a. Web Defacement;

b. DDoS;Malware;

c. Phising;

d. Pembajakan akun

e. Akses Ilegal

f. Spam

Dukungan yang diberikan oleh CSIRT-STMIKJ kepada konstituen dapat bervariasibergantung dari jenis dan dampak insiden.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

CSIRT-STMIKJ akan melakukan kerja sama dan berbagi informasi dengan CSIRT dari Kementerian dan atau Lembaga lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh CSIRT-STMIKJ akan dirahasiakan.

4.3. Komunikasi dan Autentikasi untuk komunikasi biasa CSIRT-STMIKJ dapat menggunakan alamat e-mail tanpa enkripsi data (e-mail konvensional) dan telepon.

4.4. Komunikasi terkait laporan insiden dan pertukaran informasi ancaman insiden lainnya dapat menggunakan saluran komunikasi yang disediakan (e-mail, whatsapp, call center) yang telah terenkripsi atau dilengkapi dengan kata sandi.

5. Layanan

5.1. Layanan Reaktif

Layanan reaktif dari CSIRT-STMIKJ merupakan layanan utama dan bersifatprioritas, yaitu:

5.1.1. Layanan pemberian peringatan terkait dengan laporan insiden siber Layanan ini dilaksanakan oleh CSIRT-STMIKJ berupa pemberianperingatan adanya insiden siber pada sistem elektronik dan informasistatistik yang dikelola oleh masing-masing satuan kerja Kemendikbudristek.

5.1.2. Layanan penanggulangan dan pemulihan Insiden

Layanan ini diberikan oleh CSIRT-STMIKJ berupa koordinasi, analisis, rekomendasi teknis, dan bantuan kunjungan ke lokasi dalam rangka penanggulangan dan pemulihan insiden siber. CSIRT-STMIKJ memberikaninformasi statistik terkait layanan ini.

5.1.3. Layanan penanganan kerawanan Layanan ini diberikan oleh CSIRT-STMIKJ berupa koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan (*hardening*), CSIRT-STMIKJ memberikan informasi statistik terkait layanan ini. Namun, layanan ini hanya berlaku apabila syarat-syarat berikut terpenuhi:

a. Pelapor atas kerawanan adalah pemilik sistem elektronik. Jika pelapor adalah bukan pemilik sistem, maka laporan kerawanannya tidak dapatditangani;
b. Layanan penanganan kerawanan yang dimaksud dapat juga merupakan tindak lanjut atas kegiatan *Vulnerability Assessment*.

5.1.4. Layanan penanganan artefak

Layanan ini diberikan oleh CSIRT-STMIKJ berupa penanganan artefak dalam rangka pemulihan sistem elektronik terdampak ataupun dukungan investigasi. CSIRT-STMIKJ memberikan informasi statistik terkait layanan ini

5.2. Layanan Proaktif

CSIRT-STMIKJ secara aktif membangun kapasitas sumber daya keamanan siber melalui kegiatan:

5.2.1. Pemberitahuan hasil pengamatan terkait dengan ancaman baru Layananini diberikan oleh CSIRT-STMIKJ berupa hasil dari sistem deteksi dini sistem monitoring keamanan. CSIRT-STMIKJ memberikan informasi statistik terkaitlayanan ini.

5.2.2. Layanan *security assessment*

Layanan ini diberikan oleh CSIRT-STMIKJ berupa identikasi kerentanan danpenilaian risiko atas kerentanan yang ditemukan. CSIRT-STMIKJ memberikan informasi statistik terkait layanan ini.

5.2.3. Layanan security audit

Layanan ini diberikan oleh CSIRT-STMIKJ berupa penilaian keamanan informasi. CSIRT-STMIKJ memberikan informasi statistik terkait layanan ini.

5.2.4. Layanan Manajemen

Kualitas Keamanan CSIRT-STMIKJ meningkatkan kualitas keamananmelalui kegiatan:

a. Konsultasi terkait kesiapan penanggulangan dan pemulihan Insiden
b. Layanan ini diberikan oleh CSIRT-STMIKJ berupa pemberian rekomendasi teknis berdasarkan hasil analisis terkait penanggulangan dan pemulihan insiden
c. Pembangunan kesadaran dan kepedulian terhadap keamanan siber
d. Dalam layanan ini CSIRT-STMIKJ mendokumentasikan dan mempublikasikan berbagai kegiatan yang dilakukan dalam rangka pembangunan kesadaran dan kepedulian terhadap keamanan siber
e. Pembinaan terkait kesiapan penanggulangan dan pemulihan

insiden

f. CSIRT-STMIKJ menyiapkan program pembinaan dalam rangka pendukung penanggulangan dan pemulihan insiden.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt[at]stmik.jayakarta.ac.id dengan melampirkan sekurang-kurangnya:

a. Foto/*scan* kartu identitas

b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan

7. Disclaimer terkait penanganan jenis *malware* tergantung dari ketersediaan *tools* yang dimiliki.