RFC 2350 CSIRT-UBJ

1. Informasi mengenai dokumen ini berisi deskripsi CSIRT-UBJ berdasarkan RFC 2350, yaitu informasi dasar mengenai CSIRT-UBJ, menjelaskan tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi CSIRT-UBJ.
   1.1. Tanggal update terakhir dokumen merupakan dokumen versi 1.2 yang diterbitkan pada tanggal 2 Maret 2023
   1.2. Tidak ada daftar distribusi untuk pemberitahuan mengenai pembaharuan dokumen.
   1.3. Lokasi dimana dokumen ini bisa didapat versi terbaru dari dokumen ini tersedia pada web https://csirt.ubharajaya.ac.id
   1.4. Keaslian kedua dokumen (versi bahasa inggris dan bahasa Indonesia) adalah dokumen yang telah ditanda tangani Kepala CSIRT-UBJ.
   1.5. Identifikasi dokumen kedua dokumen (versi bahasa inggris dan bahasa Indonesia) memiliki atribut yang sama, yaitu:
      1.5.1. Judul : RFC 2350 CSIRT-UBJ
      1.5.2. Versi : 1.0
      1.5.2. Tanggal Publikasi : 26 Oktober 2023
      1.5.3. Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak
   2.1. Nama Tim Computer Security Incident Response Team Universitas Bhayangkara Jakarta Raya disingkat dengan CSIRT-UBJ.
   2.2. Alamat Jl. Raya Perjuangan Bekasi Utara, Kota Bekasi, Jawa Barat 17121, Indonesia.
   2.3. Zona Waktu Jakarta (GMT+07:00)
   2.4. Nomor Telepon +62 21 88955882
   2.5. Nomor Fax +62 21 88955871
   2.6. Nomor Helpdesk CSIRT-UBJ +62 815-6031-787
   2.6. Alamat Surat Elektronik (E-mail) csirtubj[at]ubharajaya.ac.id
   2.7. Anggota Tim

Ketua CSIRT-UBJ adalah Direktur PTI dengan anggota tim adalah Sekretaris Direktir dan seluruh staf PTI UBJ dan perwakilan dari Dosen Fakultas Ilmu Komputer.

2.8. Informasi/data lain

Tidak ada.

2.9. Catatan-catatan pada Kontak CSIRT-UBJ

Metode yang disarankan untuk menghubungi CSIRT-UBJ adalah melalui e-mail pada alamat csirtubj[at]ubharajaya.ac.id atau melalui nomor telepon (+62 815-6031-787) ke CSIRT-UBJ yang siaga selama 24/7.

3. Mengenai CSIRT-UBJ

3.1. Visi CSIRT-UBJ adalah terwujudnya ketahanan siber pada sektor pendidikan yang handal dan profesional di lingkungan Universitas Bhayangkara Jakarta Raya.

3.2. Misi dari CSIRT-UBJ, yaitu:

3.2.1. Mengoordinasikan dan mengkolaborasikan layanan keamanan siber pada kampus baik internal dan eksternal di lingkungan Universitas Bhayangkara Jakarta Raya.

3.2.2. Mengidentifikasi kerentanan keamanan secara menyeluruh

3.2.3. Meningkatkan respon aspek keamanan kepada seluruh Satuan Unit Kerja di kampus Universitas Bhayangkara Jakarta Raya.

3.2.4. Meningkatkan mutu layanan TIK Pendidikan, Kebudayaan, Riset dan Teknologi dari acaman siber.

3.3. Konstituen

Konstituen CSIRT-UBJ adalah seluruh satuan unit kerja kampus UBJ.

3.4. Sponsorship dan/atau Afiliasi

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

4. Kebijakan–Kebijakan

4.1. Jenis-jenis insiden dan tingkat/level Dukungan CSIRT-UBJ memiliki otoritas untuk menangani insiden yaitu:

a. Web Defacement;

b. DDoS;

c. Malware;
d. Phising;
e. Pembajakan akun
f. Akses Ilegal
g. Spam

Dukungan yang diberikan oleh CSIRT-UBJ kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

4.3. Komunikasi dan Autentikasi untuk komunikasi biasa CSIRT-UBJ 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-UBJ merupakan layanan utama dan bersifat prioritas, yaitu:

5.1.1. Layanan pemberian peringatan terkait dengan laporan insiden siber

Layanan ini dilaksanakan oleh CSIRT-UBJ berupa pemberian peringatan adanya insiden siber pada sistem elektronik dan informasi statistik yang dikelola oleh masing-masing satuan kerja Kemendikbudristek

5.1.2. Layanan penanggulangan dan pemulihan Insiden

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

5.1.3. Layanan penanganan kerawanan

Layanan ini diberikan oleh CSIRT-UBJ berupa koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan (*hardening*), CSIRT-UBJ 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 dapat ditangani;
b. Layanan penanganan kerawanan yang dimaksud dapat juga merupakan tindak lanjut atas kegiatan *Vulnerability Assessment*.

5.1.4. Layanan penanganan artifak

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

5.2. Layanan Proaktif

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

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

5.2.2. Layanan security assessment

Layanan ini diberikan oleh CSIRT-UBJ berupa identikasi kerentanan dan penilaian risiko atas kerentanan yang ditemukan. CSIRT-UBJ memberikan informasi statistik terkait layanan ini.

5.2.3. Layanan security audit

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

5.2.4. Layanan Manajemen

Kualitas Keamanan CSIRT-UBJ meningkatkan kualitas keamanan melalui kegiatan:

a. Konsultasi terkait kesiapan penanggulangan dan pemulihan Insiden

b. Layanan ini diberikan oleh CSIRT-UBJ 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-UBJ 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-UBJ menyiapkan program pembinaan dalam rangka pendukung penanggulangan dan pemulihan insiden

6. Pelaporan Insiden

   Laporan insiden keamanan siber dapat dikirimkan ke csirtubj[at]ubharajaya.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.