RFC 2350
UNUJA-CSIRT
Computer Security Incident Response Team
Universitas Nurul Jadid

Nama Tim	**UNUJA-CSIRT**
Versi Dokumen	1.0
Tanggal Publikasi	25 Febuari 2026
Bahasa	Bahasa Indonesia
Status	Aktif
Berlaku Hingga	Sampai versi terbaru diterbitkan
URL Dokumen	https://csirt.unuja.ac.id/rfc2350.pdf

1. Informasi Mengenai Dokumen

Dokumen ini berisi deskripsi UNUJA-CSIRT (Computer Security Incident Response Team Universitas Nurul Jadid) berdasarkan RFC 2350 -- standar internasional "Expectations for Computer Security Incident Response". Dokumen menjelaskan informasi dasar, tanggung jawab, layanan, dan cara menghubungi UNUJA-CSIRT.

1.1. Tanggal Update Terakhir

Dokumen ini adalah versi 1.0, diterbitkan pada 25 Febuari 2026.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi khusus. Setiap pembaruan akan diumumkan melalui laman resmi UNUJA-CSIRT di https://csirt.unuja.ac.id.

1.3. Lokasi Dokumen

Dokumen tersedia pada:

- https://csirt.unuja.ac.id/rfc2350.pdf (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Dokumen telah ditandatangani secara digital menggunakan PGP Key milik UNUJA-CSIRT guna menjamin keaslian dan integritas. Informasi kunci publik tersedia pada Subbab 2.8.

1.5. Identifikasi Dokumen

Judul	**RFC 2350 UNUJA-CSIRT**
Versi	1.0
Tanggal Publikasi	1 Januari 2025
Kedaluwarsa	Valid hingga versi terbaru dipublikasikan

2. Informasi Data / Kontak

2.1. Nama Tim

Nama Lengkap: UNIVERSITAS NURUL JADID – COMPUTER SECURITY INCIDENT RESPONSE TEAM

Singkatan: UNUJA-CSIRT

2.2. Alamat

Pusat Data dan Sistem Informasi

Universitas Nurul Jadid

Jl. KH. Zaini Mun'im, Karanganyar, Paiton

Probolinggo, Jawa Timur 67291 – Indonesia

2.3. Zona Waktu

Waktu Indonesia Barat (WIB) – GMT+07:00

2.4. Nomor Telepon

Hotline Darurat: 0888 30 77077

2.5. Nomor Fax

-

2.6. Telekomunikasi Lain

WhatsApp (jam kerja Sabtu0888 30 77077Kamis 08.00–15.00 WIB): tersedia via hotline darurat

2.7. Alamat Surat Elektronik (Email)

csirt[at]unuja[dot]ac[dot]id

Formulir online: https://csirt.unuja.ac.id/lapor-insiden

2.8. Kunci Publik (Public Key) dan Informasi Enkripsi

UNUJA-CSIRT menggunakan enkripsi PGP untuk komunikasi rahasia.

URL Public Key	**https://csirt.unuja.ac.id/publickey.asc**
Bits	4096
Key ID	Tersedia di laman resmi UNUJA-CSIRT
Key Fingerprint	Tersedia di laman resmi UNUJA-CSIRT

2.9. Anggota Tim

Ketua UNUJA-CSIRT adalah Kepala Pusat Data dan Sistem Informasi Universitas Nurul Jadid. Anggota tim terdiri dari seluruh staf Divisi Keamanan Siber dan Jaringan di lingkungan Pusat Data dan Sistem Informasi UNUJA.

2.10. Informasi Lain

Informasi lebih lanjut tersedia di laman resmi: https://csirt.unuja.ac.id

2.11. Catatan Kontak UNUJA-CSIRT

Metode yang disarankan untuk menghubungi UNUJA-CSIRT:

- Email: csirt[at]unuja[dot]ac[dot]id (untuk laporan, konsultasi, dan komunikasi umum)
- Formulir pengaduan online: https://csirt.unuja.ac.id/lapor-insiden
- Hotline darurat: 0888 30 77077 (untuk insiden kritis yang membutuhkan respons segera)

3. Mengenai UNUJA-CSIRT

3.1. Visi

> ***"****Mewujudkan Universitas Nurul Jadid sebagai kampus dengan ketahanan siber yang handal, profesional, dan berkarakter islami – menjaga kedaulatan data dan resiliensi SPBE di era integrasi digital.****"***

3.2. Misi

Misi UNUJA-CSIRT:

- Menjaga keamanan jaringan komputer dan sistem informasi di lingkungan Universitas Nurul Jadid dengan mencegah serangan siber serta merespons dengan cepat dan tepat ketika terjadi insiden.
- Menyelenggarakan Triase insiden yang terukur: isolasi server terinfeksi Malware, Ransomware, atau defacement web agar tidak menyebar ke jaringan fakultas lain.
- Melaksanakan Audit & VAPT (Vulnerability Assessment and Penetration Testing) secara proaktif sebelum aplikasi mahasiswa atau unit di deploy ke lingkungan produksi (Go-Live).
- Mengelola program Vulnerability Disclosure Program (VDP) sebagai kanal resmi pelaporan celah keamanan dari pihak eksternal.
- Menyediakan Security Advisory berupa edukasi tren Zero-Day, panduan literasi digital, dan repositori edukasi keamanan bagi seluruh sivitas akademika.
- Mengembangkan kebijakan dan prosedur keamanan informasi yang komprehensif untuk melindungi data dan informasi penting di lingkungan UNUJA.
- Berkoordinasi dengan CSIRT nasional dan internasional untuk berbagi informasi dan sumber daya dalam menghadapi ancaman keamanan siber.
- Mengintegrasikan nilai-nilai islami dalam setiap aspek pengelolaan keamanan siber sebagai wujud komitmen UNUJA sebagai perguruan tinggi berbasis pesantren.

3.3. Konstituen

Konstituen UNUJA-CSIRT adalah seluruh civitas akademika Universitas Nurul Jadid, meliputi:

- Mahasiswa aktif Universitas Nurul Jadid
- Dosen dan tenaga pengajar
- Tenaga kependidikan dan staf administrasi
- Pimpinan dan manajemen universitas
- Unit kerja, lembaga, dan badan di bawah naungan UNUJA
- Mitra dan pihak eksternal yang memiliki akses ke sistem informasi UNUJA

3.4. Sponsorship dan/atau Afiliasi

Pendanaan operasional UNUJA-CSIRT bersumber dari Anggaran Universitas Nurul Jadid. UNUJA-CSIRT berkoordinasi dengan:

- BSSN (Badan Siber dan Sandi Negara) Republik Indonesia

- ID-CSIRT (Indonesia Computer Security Incident Response Team)
- Forum CSIRT Perguruan Tinggi Indonesia
- Komunitas keamanan siber nasional

3.5. Otoritas

UNUJA-CSIRT memiliki kewenangan untuk:

- Melakukan penanggulangan, mitigasi, dan triase insiden keamanan siber di lingkungan UNUJA
- Melaksanakan audit keamanan & VAPT terhadap seluruh sistem elektronik UNUJA
- Melakukan investigasi dan analisis dampak insiden keamanan siber
- Melakukan pemulihan pasca insiden keamanan siber
- Mengeluarkan Security Advisory, peringatan, dan rekomendasi keamanan
- Mengelola program VDP (Vulnerability Disclosure Program)
- Berkoordinasi dengan pihak eksternal dalam penanganan insiden

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat Dukungan

UNUJA-CSIRT melayani penanganan insiden keamanan siber berikut:

No	Jenis Insiden	Deskripsi
1	Web Defacement	Perusakan tampilan halaman website milik UNUJA oleh pihak tidak berwenang
2	DDoS / DoS	Serangan yang menyebabkan gangguan atau kelumpuhan layanan sistem informasi UNUJA
3	Malware	Infeksi perangkat lunak berbahaya pada sistem/perangkat di lingkungan UNUJA
4	Ransomware	Serangan enkripsi data yang meminta tebusan pada aset digital UNUJA
5	Phishing	Upaya penipuan yang menyamar sebagai entitas UNUJA untuk mencuri informasi sensitif
6	Pembajakan Akun	Pengambilalihan akun sistem informasi UNUJA oleh pihak tidak berwenang
7	Akses Ilegal	Upaya atau keberhasilan akses tidak sah ke sistem, jaringan, atau data UNUJA
8	Spam	Penyebaran pesan massal tidak diinginkan via infrastruktur UNUJA

9	Kebocoran Data	Eksposur data sensitif civitas akademika atau data institusi UNUJA
10	SQL Injection / RCE	Eksploitasi celah injeksi atau Remote Code Execution pada aplikasi UNUJA

Tingkat dukungan yang diberikan bervariasi berdasarkan jenis dan dampak insiden. UNUJA-CSIRT menerapkan pendekatan Triase untuk memprioritaskan penanganan.

4.2. Kerja Sama, Interaksi, dan Pengungkapan Informasi

UNUJA-CSIRT menjalin kerja sama dan berbagi informasi dengan CSIRT atau organisasi keamanan siber terkait dalam penanganan insiden. Seluruh informasi yang diterima dijaga kerahasiaannya sesuai kebijakan privasi dan keamanan informasi UNUJA.

Pengungkapan informasi kepada pihak ketiga hanya dilakukan apabila:

- Diperlukan untuk penanganan insiden yang sedang berlangsung
- Diwajibkan oleh peraturan perundang-undangan yang berlaku di Indonesia
- Mendapat persetujuan dari pimpinan yang berwenang di UNUJA

4.3. Komunikasi dan Autentikasi

Komunikasi dengan UNUJA-CSIRT dapat dilakukan melalui:

- Email konvensional (tanpa enkripsi) – untuk komunikasi umum dan informasi tidak sensitif
- Email terenkripsi PGP untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia
- Telepon – untuk komunikasi darurat yang membutuhkan respons segera
- Formulir online terenkripsi via https://csirt.unuja.ac.id/lapor-insiden

Channel email merupakan jalur resmi utama untuk pelaporan insiden.

5. Layanan

UNUJA-CSIRT menyelenggarakan layanan dalam dua kategori: Layanan Utama (Reaktif) dan Layanan Tambahan (Proaktif & Edukatif).

5.1. Layanan Utama

5.1.1. Manajemen Insiden (Reaktif)

Layanan inti respons insiden siber dengan pendekatan Triase yang terukur. Proses penanganan meliputi:

1. Identifikasi & Triase: Mengidentifikasi, memverifikasi, dan menetapkan tingkat keparahan insiden. Melakukan triase cepat untuk mengisolasi sistem terinfeksi (Malware, Ransomware, Web Defacement) agar tidak menyebar ke jaringan fakultas lain.

2. Response Insiden: Merespons dengan cepat sesuai tingkat keparahan, termasuk isolasi sistem, revokasi akses, dan patching darurat.
3. Investigasi: Melakukan analisis forensik untuk menentukan penyebab, ruang lingkup kerusakan, dan dampak terhadap sistem dan data.
4. Pemberitahuan: Menginformasikan insiden kepada pihak terkait (pengguna, manajemen, regulator jika diperlukan) sesuai klasifikasi TLP (Traffic Light Protocol).
5. Pemulihan: Memulihkan sistem dan data terdampak ke kondisi aman dan normal, memastikan integritas layanan kembali terjamin.
6. Evaluasi & Perbaikan: Melakukan post-incident review dan memperbaiki kebijakan/prosedur agar insiden serupa tidak terulang.

5.1.2. Pemberian Peringatan Terkait Keamanan Siber

UNUJA-CSIRT memberikan peringatan dini kepada seluruh stakeholder di lingkungan UNUJA mengenai adanya potensi ancaman, kerentanan, dan insiden siber. Peringatan disampaikan memperhatikan tanggung jawab masing-masing stakeholder melalui email, portal resmi, dan media sosial resmi UNUJA-CSIRT.

5.2. Layanan Tambahan (Proaktif)

5.2.1. Audit & VAPT (Vulnerability Assessment and Penetration Testing)

Assessment keamanan yang dilakukan secara proaktif sebelum aplikasi mahasiswa, unit, atau fakultas dideploy ke lingkungan produksi (Go-Live). Layanan ini bertujuan memblokir celah injeksi (SQL Injection), Remote Code Execution (RCE), dan kerentanan kritis lainnya sebelum sistem diekspos ke publik.

- Vulnerability Assessment: Identifikasi dan penilaian risiko kerentanan pada aset TI UNUJA
- Penetration Testing: Simulasi serangan terkontrol untuk memvalidasi efektivitas kontrol keamanan
- Security Review Go-Live: Audit wajib sebelum aplikasi baru masuk produksi

5.2.2. Security Advisory & Vulnerability Disclosure Program (VDP)

Program edukasi dan kanal resmi pelaporan celah keamanan bagi sivitas akademika dan pihak eksternal:

- Security Advisory: Edukasi tren ancaman Zero-Day, panduan keamanan terkini, dan repositori literasi digital untuk seluruh sivitas akademika UNUJA
- Vulnerability Disclosure Program (VDP): Program formal yang memungkinkan peneliti keamanan dan komunitas eksternal melaporkan celah keamanan secara bertanggung jawab (Responsible Disclosure) tanpa ancaman sanksi
- Advisory Bulletin: Publikasi berkala mengenai ancaman siber yang relevan dengan lingkungan akademik

5.2.3. Penanganan Kerawanan Sistem Elektronik

Layanan koordinasi, analisis, dan rekomendasi teknis penguatan keamanan (hardening) sistem elektronik UNUJA. Layanan berlaku dengan syarat:

- Pelapor kerawanan adalah pemilik sistem elektronik yang bersangkutan
- Layanan dapat merupakan tindak lanjut dari kegiatan Vulnerability Assessment dan VAPT

5.2.4. Penanganan Artefak Digital

Pengumpulan, analisis, dan pengelolaan artefak digital dalam rangka pemulihan sistem elektronik yang terdampak maupun dukungan investigasi. UNUJA-CSIRT menyediakan informasi statistik terkait layanan di lingkungan UNUJA.

5.2.5. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Informasi mengenai potensi ancaman dan pembaruan keamanan siber dikomunikasikan kepada seluruh sivitas akademika UNUJA (mahasiswa, dosen, tenaga kependidikan, dan mitra eksternal terkait) dengan menerapkan Traffic Light Protocol (TLP):

TLP: RED	Hanya untuk tim internal UNUJA-CSIRT dan penerima yang ditentukan
TLP: AMBER	Untuk konstituen internal UNUJA yang membutuhkan informasi
TLP: GREEN	Untuk komunitas dan ekosistem akademik UNUJA
TLP: WHITE	Informasi publik, dapat disebarluaskan bebas

5.2.6. Pendeteksian Serangan

Layanan pendeteksian serangan menggunakan infrastruktur keamanan yang dimiliki UNUJA, meliputi:

- Firewall – perlindungan perimeter jaringan 100%
- Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)
- Monitor server real-time (Live) untuk deteksi anomali aktivitas jaringan
- Security Information and Event Management (SIEM) untuk analisis log terpusat

5.2.7. Analisis Risiko Keamanan Siber

Layanan analisis risiko dilakukan menggunakan berbagai sumber data yang dimiliki Pusat Data dan Sistem Informasi UNUJA, mencakup:

- Identifikasi dan inventarisasi aset TI kritis
- Penilaian ancaman dan kerentanan
- Analisis dampak dan kemungkinan risiko
- Rekomendasi mitigasi risiko

5.2.8. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Layanan konsultasi kesiapan penanganan insiden bagi stakeholder UNUJA, mencakup evaluasi kebijakan keamanan, prosedur respons insiden, dan rekomendasi peningkatan kapabilitas keamanan siber. Layanan diberikan berdasarkan permintaan unit atau pemangku kepentingan.

5.2.9. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

UNUJA-CSIRT secara aktif membangun budaya keamanan siber melalui:

- Pelatihan dan workshop keamanan siber (tatap muka & daring)
- Seminar, webinar, dan FGD terkait ancaman siber terkini
- Repositori panduan dan artikel edukasi di portal UNUJA-CSIRT
- Kampanye kesadaran siber via media sosial resmi UNUJA
- Simulasi dan drill penanganan insiden (tabletop exercise)
- Integrasi materi keamanan siber dalam kurikulum program studi relevan
- Edukasi tren Zero-Day dan ancaman emerging threat secara berkala

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan kepada UNUJA-CSIRT melalui:

Saluran	Keterangan
Email	csirt[at]unuja[dot]ac[dot]id (jalur resmi utama)
Formulir Online	https://csirt.unuja.ac.id/lapor-insiden
Hotline Darurat	0888 30 77077 (jam kerja, untuk insiden kritis)

Setiap laporan insiden wajib menyertakan sekurang-kurangnya:

- Foto atau scan kartu identitas pelapor (KTP / KTM / ID Karyawan UNUJA)
- Bukti insiden: foto, screenshot, atau log file yang ditemukan
- Deskripsi singkat insiden: tanggal, waktu, sistem yang terdampak, kronologi kejadian
- Nama, jabatan/status, nomor telepon, dan alamat email pelapor
- Langkah-langkah yang telah diambil sebelum melapor (jika ada)

UNUJA-CSIRT akan memberikan konfirmasi penerimaan laporan dalam 1x24 jam hari kerja dan melakukan penanganan sesuai tingkat keparahan insiden menggunakan pendekatan Triase.

7. Disclaimer

Penanganan insiden keamanan siber oleh UNUJA-CSIRT bergantung pada ketersediaan sumber daya, perangkat, dan kapabilitas teknis yang dimiliki Universitas Nurul Jadid pada saat insiden terjadi.

UNUJA-CSIRT tidak bertanggung jawab atas:

- Kerugian yang timbul akibat keterlambatan penanganan yang disebabkan faktor di luar kendali UNUJA-CSIRT
- Kerusakan atau kehilangan data yang terjadi sebelum insiden dilaporkan
- Insiden yang terjadi pada sistem atau perangkat di luar lingkup konstituen UNUJA-CSIRT
- Kerugian yang timbul akibat kegagalan pengguna mengikuti panduan keamanan yang telah diterbitkan

UNUJA-CSIRT berkomitmen memberikan layanan terbaik dalam batas kemampuan dan sumber daya yang tersedia demi menjaga keamanan ekosistem digital Universitas Nurul Jadid.