

RFC 2350 PKC-CSIRT

1. Informasi Mengenai Dokumen

Dokumen ini berisi deskripsi *PKC-CSIRT* berdasarkan RFC 2350, yaitu informasi dasar mengenai *PKC-CSIRT*, menjelaskan tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi *PKC-CSIRT*.

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 01 Desember

1.2. Daftar Distribusi untuk Pemberitahuan

Seluruh Konstituen PKC-CSIRT.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :

<https://tautan.online> (link download dokumen) ditempatkan di website feature download dokumen RFC

1.4. Keaslian Dokumen

Dokumen ini telah ditandatangani oleh ketua PKC-CSIRT

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 *PKC-CSIRT*;

Versi : 1.0;

Tanggal Publikasi : (*tanggal penandatanganan dokumen ini*);

Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

PT. Pupuk Kujang – Computer Security Incident Response Team

Disingkat : *PKC-CSIRT*.

2.2. Alamat

Jl. Jend. A. Yani No.39 Cikampek, Kab. Karawang, Jawa Barat

2.3. Zona Waktu

Indonesia (GMT+7)

2.4. Nomor Telepon

(+62-264) 316 141 & 317 007

2.5. Nomor Fax

(+62-22)

2.6. Telekomunikasi Lain

	Nama narahubung 1:	Herlambang Adi Budiman
	Nomor telepon/ <i>Handphone</i> :	081316193349
	Alamat email:	herlambangadi[at]pupuk-kujang.co.id
	Nama narahubung 2:	Herlambang Adi Budiman
	Nomor telepon/ <i>Handphone</i> :	081316193349
	Alamat email:	herlambangadi[at]pupuk-kujang.co.id

2.7. Alamat Surat Elektronik (*E-mail*)

[pkc.csirt\[at\]pupuk-kujang.co.id](mailto:pkc.csirt[at]pupuk-kujang.co.id)

2.8. Kunci Publik (*Public Key*) dan Informasi/Data Enkripsi lain

(email client thunderbird) File PGP key ini tersedia pada:

<https://csirt.pupuk-kujang.co.id>

(ada 2 link, 1 untuk download dokumen RFS dan link public key dari email PKC-CSIRT)

2.9. Anggota Tim

Ketua PKC-CSIRT	: VP Teknologi Informasi PKC
Sekretaris PKC-CSIRT	: Officer Perencanaan dan Tatakelola TI
Narahubung	: Jr Officer Infrastruktur & Layanan TI
Koordinator Infrastruktur & Layanan	: AVP Infrastruktur & Layanan TI
Tim Insiden Respon	: Staf Fungsional Layanan TI
Tim Penanggulangan dan Pemulihan Infrastruktur	: Staf Fungsional Infrastruktur TI
Koordinator Aplikasi	: Officer Digitalisasi
Tim Keamanan Aplikasi	: Staf Fungsional Digitalisasi

2.10. Informasi/Data lain

N/A.

2.11. Catatan-catatan pada Kontak *NAMA-CSIRT*

Metode yang disarankan untuk menghubungi *PKC-CSIRT* adalah melalui *e-mail* pada alamat [pkc.csirt\[at\]pupuk-kujang.co.id](mailto:pkc.csirt[at]pupuk-kujang.co.id) atau melalui nomor telepon yang tercantum pada Informasi Data/Kontak. Pada hari Senin-Jumat pada pukul 07.00-

16.00 WIB dan jika terdapat hal-hal yang mendesak di luar jam tersebut dapat dilakukan penanganan.

3. Mengenai PKC-CSIRT

3.1. Visi

Visi *PKC-CSIRT* adalah menjadi komponen utama untuk tercapainya Visi Perusahaan dengan meningkatkan ketahanan siber di sektor industri pupuk

3.2. Misi

Perwujudan visi sebagaimana dituangkan di atas akan dicapai melalui upaya-upaya yang terkandung dalam misi *PKC-CSIRT*, yaitu :

- a. Mengkoordinasikan dan mengkolaborasikan layanan keamanan siber di lingkungan Perusahaan dan pemangku kepentingan.
- b. Membangun kemampuan dan kapasitas sumber daya keamanan di sektor industri pupuk
- c. Membangun kerjasama dalam rangka penanggulangan dan pemulihan insiden keamanan siber di lingkungan industri agrokimia Indonesia

3.3. Konstituen

Konstituen *PKC-CSIRT* meliputi seluruh pengguna yang menggunakan layanan sistem informasi, meliputi karyawan sistem informasi perusahaan, aset informasi, yang memiliki keterkaitan langsung dengan layanan dan sistem PT Pupuk Kujang. *PKC-CSIRT* berperan sebagai otoritas internal perusahaan dalam koordinasi, penanganan, dan pelaporan insiden keamanan siber sesuai ketentuan peraturan perundang-undangan yang berlaku.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan *PKC-CSIRT* bersumber dari anggaran internal Perusahaan, Departemen Teknologi Informasi PKC

3.5. Otoritas

Berdasarkan Kebijakan Pengelolaan Sistem dan Teknologi Informasi dan Kebijakan Pengelolaan Keamanan Informasi, *PKC-CSIRT* memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi, dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber pada sektor industri pupuk.

4. Kebijakan – Kebijakan

Seluruh informasi insiden diklasifikasikan dan dikelola sesuai prinsip kerahasiaan, integritas, dan ketersediaan (CIA), serta hanya dapat diungkapkan kepada pihak yang berwenang sesuai ketentuan hukum dan kebijakan perusahaan.

4.1. Jenis-jenis Insiden dan Tingkat/Level Dukungan

PKC-CSIRT memiliki otoritas untuk menangani insiden yaitu :

- a. Web Defacement;

- b. DDOS;
- c. Malware;
- d. Phising;
- e. Kebocoran data dan/atau pelanggaran kerahasiaan informasi;
- f. Akses tidak sah (*unauthorized access*) terhadap sistem dan jaringan;
- g. Penyalahgunaan akun dan kredensial (*account compromise*);

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

PKC-CSIRT akan melakukan kerja sama dan berbagi informasi dengan CSIRT atau organisasi lain dalam lingkup keamanan siber dengan tetap menjunjung tinggi prinsip kerahasiaan, di mana seluruh informasi yang diterima dikelola dan dilindungi sesuai ketentuan yang berlaku. Dalam hal terjadi insiden keamanan siber yang berdampak signifikan, *PKC-CSIRT* akan melakukan koordinasi dan pelaporan kepada BSSN dan/atau CSIRT nasional sesuai dengan peraturan dan mekanisme yang ditetapkan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa *PKC-CSIRT* Indonesia dapat menggunakan alamat e-mail tanpa enkripsi data (e-mail konvensional) dan telepon. Namun, untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi PGP pada e-mail.

5. Layanan

Layanan *PKC-CSIRT* diberikan berdasarkan tingkat prioritas dan dampak insiden, dengan memperhatikan kapasitas sumber daya dan kebijakan internal perusahaan.

5.1. Layanan Utama

Layanan utama dari *PKC-CSIRT* yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini dilaksanakan oleh *PKC-CSIRT* berupa pemberian peringatan adanya insiden siber kepada pihak yang berkepentingan.

5.1.2. Penanganan Insiden Siber

Layanan ini diberikan berupa kegiatan menerima, menanggapi, dan menganalisis Insiden Siber.

5.2. Layanan Tambahan

Layanan tambahan dari *PKC-CSIRT* merupakan layanan yang bersifat preventif dan proaktif dalam rangka penguatan ketahanan keamanan siber perusahaan, yang meliputi::

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini melibatkan identifikasi, evaluasi dan penanganan terhadap kerawanan atau celah keamanan yang ada dalam sistem elektronik

perusahaan. Tujuannya adalah untuk mengurangi risiko keamanan dengan memperbaiki atau mengatasi kerawanan yang terdeteksi.

Secara umum penanganan ini dibagi menjadi:

- i. Pelaporan kerawanan yang bersifat sewaktu oleh pemilik/penyelenggara sistem elektronik milik pihak terkait.
- ii. Penanganan kerawanan sebagai tindak lanjut dari kegiatan audit atau vulnerability assessment.

5.2.2. Penanganan Artefak Digital.

Layanan ini mencakup proses pengumpulan, analisis, dan interpretasi terhadap artefak digital yang terkait dengan insiden keamanan. Hal ini dapat mencakup data forensik, jejak serangan, dan bukti elektronik lainnya untuk mendukung investigasi dan penanganan insiden.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini melibatkan pemberian informasi tentang potensiancaman keamanan yang teridentifikasi atau diamati oleh tim *PKC-CSIRT*. Pemberitahuan ini bertujuan untuk memberi peringatan dini kepada pihak yang berkepentingan agar mereka dapat mengambil tindakan preventif yang sesuai.

5.2.4. Pendekstrian Serangan

Layanan ini fokus pada pendekstrian awal terhadap serangan keamanan yang mungkin terjadi di lingkungan perusahaan. Tim *PKC-CSIRT* akan menggunakan teknologi dan metode tertentu untuk mengenali tanda-tanda aktivitas mencurigakan atau serangan yang sedang berlangsung.

5.2.5. Analisis Risiko Keamanan Siber.

Layanan ini melibatkan evaluasi terhadap risiko keamanan siber yang dihadapi oleh perusahaan, termasuk identifikasi potensi ancaman, kerentanan, dan dampaknya terhadap bisnis. Analisis ini membantu dalam pengembangan strategi mitigasi risiko yang efektif.

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Layanan ini menyediakan konsultasi kepada pihak-pihak terkait dalam hal persiapan dan kesiapan dalam menangani insiden keamanan siber. Tim *PKC-CSIRT* akan memberikan saran dan bimbingan untuk meningkatkan kapasitas dan responsibilitas terhadap keamanan siber.

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap

Layanan ini bertujuan untuk meningkatkan pemahaman dan kesadaran seluruh anggota organisasi terkait dengan risiko keamanan siber. Ini termasuk penyuluhan, pelatihan, dan kampanye kesadaran yang dirancang untuk mengurangi insiden yang disebabkan oleh kesalahan manusia dan meningkatkan budaya keamanan siber di perusahaan.

6. Pelaporan Insiden

Setiap laporan insiden akan dicatat, didokumentasikan, dan disimpan sebagai bagian dari evidence penanganan insiden keamanan siber perusahaan.

Laporan insiden keamanan siber dapat dikirimkan ke [pkc.csirt\[at\]pupuk-kujang.co.id](mailto:pkc.csirt[at]pupuk-kujang.co.id) dengan melampirkan Formulir Aduan Insiden Siber yang sekurang-kurangnya memuat :

- a. Identitas Pelapor;

- b. Tipe Laporan;
- c. Waktu Terjadinya Insiden;
- d. Tipe Insiden;
- e. Deskripsi Insiden disertai Bukti (screenshoot, domain name, URL, email dll).
- f. Atau sesuai dengan ketentuan lain yang berlaku

7. Disclaimer

PKC-CSIRT melaksanakan tugas dan fungsinya sesuai dengan kewenangan, kebijakan internal perusahaan, serta ketentuan peraturan perundang-undangan yang berlaku. *PKC-CSIRT* tidak bertanggung jawab atas insiden keamanan siber yang terjadi di luar kewenangan, di luar lingkup sistem elektronik dan/atau aset informasi yang dikelola oleh PT Pupuk Kujang, atau yang disebabkan oleh faktor di luar kendali perusahaan.

Cikampek, 30 Desember 2025

Jojok Satriadi