RFC 2350 DSF-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 18 September 2026.

1.2. Daftar Distribusi untuk Pemberitahuan

Apabila terdapat pembaruan dokumen ini maka akan didistribusikan ke seluruh pihak yang terkait dengan Perusahaan DSF-CSIRT.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://www.dipostar.com/csirt-rfc2350.pdf

1.4. Keaslian Dokumen

Dokumen telah ditandatangani oleh Ketua DSF-CSIRT.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 DSF-CSIRT[;
Versi	: 1.0;
Tanggal Publikasi	: 30 September 2026;
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Dipo Star Finance - Computer Security Incident Response Team
Disingkat: DSF-CSIRT

2.2. Alamat

Sentral Senayan 2, Lantai 3 Jl. Asia Afrika No. 8 Senayan Jakarta 10270.

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

(021) 57954100

2.5. Nomor Fax

-

2.6. Telekomunikasi Lain

-

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

dsf.csirt@dipostar.com

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

Bits : 2048 (2,048-bit RSA)
ID : 13A8 1B2A D833 BA79
Key Fingerprint : D3F5 3C80 8047 E037 B052 7C71 13A8 1B2A D833 BA79

Blok PGP Public Key

-----BEGIN PGP PUBLIC KEY BLOCK-----
mQENBGqaoIQBCADZTN9VIGflHmTWx22+J5foSEChAY5giizcyRCiUjYLtDjI6qSp
ZL5OtpzQeeb4CrZvMhIlrwDzMgo+RIWsZuMoGUdT7MI2KFxZBDTkhdPMonw2eEj8
HfUaPIEshBuJBaEbcQ0fLAxWnDwcdoVTnKH/nLB5wpIHd8jWiGFSzrqdj+Ojz0XY
BFHEv3zWl/i7IxQM6DJ6ONOhFZ63vM6sOC+7EAGMbVsuza6597x6gEzXw+hNf/6j
7gzg+oVJpTkwBsVJCWNGFiObjH5NcdCiwCa2wxe/hYS8GktuEtVHwn+HeXhzT23n
Ea3ttXSurRz8XVAxm99M7+lRjTf81IxoazW/ABEBAAG0IkRTRiBDU0ISVCA8ZHNm
LmNzaXJ0QGRpcG9zdGFyLmNvbT6JAXMEEwEIAF0WIQTT9TyAgEfgN7BSfHETqBsq
2DO6eQUCapqghBsUgAAAAAAEAA5tYW51MiwyLjUrMS4xMiwyLDECGwMFCQHg40
wF
CwkIBwICIgIGFQoJCAsCBBYCAwECHgcCF4AACgkQE6gbKtgzunmV2Af+PSeqnn7J
OARkJk9U3RxPY4cmP/obQF5BLcR3IhigNBCaMFCluCtznAKSjOU2Ur95krB/XqXu
oWBv3v5ayYtIC06aSIcdCxgZOUc9DPlf+bS9hLZIL31kOqZtSCNx8DZMyvptx2En
qEbU2IDyGgdKAI4NqHOGOZLqWlBbHbTVHx6nPO4sL9ZQR76IcmjIlhWeuiI2Bv3G
JuJinJSvAYVMOoRAROE34MpkQJjG6iADWfKO/XU9RlyhRi0jz99sh2zMO8qOgW+3
qmeTifwApZOod/77mZUOTm4sC0qtMfwd1J5Sa5sQ1JVOzhpCcXsJiXPAK6D0uuua
N2Agu+wPZ8ey67kBDQRqmqCEAQgAyf7QYll+u3BJ9DW/D1IFZbZH9vEidImUycnA
X4NmEA0jciFQzw7Om+nWTswYQsU/gr4XtdwQqlUQS0c9tFhGUmqr+KCg4tF5t7Q0
Y9wJgZKDKHAPBdWE2+ptEsmilXGa4TeRMwdSowOkXSReatlej8c3urfjUXnPqjuU
yA7mll0GdoCVpta92foLA7GgrtwlTNBxBFekirib4yMkrvZSyLAUqP8acF1LLwsM
cuKwvzltaltG3v9q5My8YKRkz0bdds54M81vt1F1XOtCFw78j0oho9aDJKzQ/md+
3J00TjlszujKWEAy8O/0yFvtuqQZ9+E+tMg+gfodPbyYPuscoQARAQABiQFYBBgB
CABCFiEE0/U8glBH4DewUnxxE6gbKtgzunkFAmqaolQbFIAAAAAABAAObWFudTIs
Mi41KzEuMTIsMiwxAhsMBQkB4ONMAAoJEBOoGyrYM7p5STcH/1reEP9DgDf7pzbd
Gf58Qj5S1e+UbVuLK8ErUhpO658CZ9YBGuvM9PU01IAvY01UCfa6wo+ONJvaroBz
Ycd84iqM7YXdzVcdZFKTRoyZReMZu5zQzOa4nDDxkvoeKZ/fq+Tt3g/CPPBVahhK
WqtgL6IKr0aEvXPMZGdBML6tHW/OJqDTFw4tjEEqaFrpcJAyYPlzzV0wbdbW+SRP
pjLzVQmn5vm4Zrww1i5gs6KESVtYPVZCahPltQo5+sBmQvxAn6zCYHIPXjZy3R+E
9cKdaRv9L6pge+9TlDv/rDUGFgfpWftbBQI+GRWGjLO+DvvXTBalJyks/nBpVoOB
kvBmCF8= =a3Mj -----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://www.dipostar.com/csirt-rfc2350.pdf

2.9. Anggota Tim

Ketua DSF-CSIRT dijabat oleh Kepala Departemen IT Operation PT Dipo Star Finance (DSF), yang ditunjuk oleh Presiden Direktur dan Chief Information Officer (CIO). Untuk detail susunan organisasi dan keanggotaan DSF-CSIRT mengacu pada Surat Keputusan DSF Nomor 0015A/ITD-DSF/06/2026 tentang Penetapan dan Piagam Tim Tanggap Insiden Siber (TTIS) atau *Establishment and Charter of Competer Security Incident Response Team* (CSIRT).

2.10. Informasi/ Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak DSF-CSIRT

Metode yang disarankan untuk menghubungi DSF-CSIRT adalah melalui e-mail pada alamat dsf.csirt@dipostar.com

3. Mengenai DSF-CSIRT

3.1. Visi

Visi DSF-CSIRT adalah menjadi Tim Tanggap Insiden Siber yang profesional, responsif, dan andal dalam menjaga keamanan informasi, memperkuat ketahanan siber, serta mendukung keberlangsungan operasional DSF.

3.2. Misi

Misi DSF-CSIRT adalah melakukan pencegahan, penanganan, dan pemulihan terhadap insiden keamanan siber guna menjaga keberlangsungan operasional DSF.

3.3. Konstituen

Konstituen DSF-CSIRT meliputi seluruh unit kerja pengguna teknologi informasi di lingkungan DSF.

3.4. Sponsorship dan/ atau Afiliasi

Pendanaan pelaksanaan tugas DSF-CSIRT bersumber dari Anggaran Departemen IT DSF.

3.5. Otoritas

DSF-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber pada organisasi DSF.

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/ Level Dukungan

DSF-CSIRT memberikan dukungan penanganan insiden keamanan siber kepada konstituen berdasarkan jenis, tingkat keparahan, dampak, urgensi, dan cakupan insiden. Jenis insiden yang ditangani meliputi, tetapi tidak terbatas pada:

a. Denial of Service (DoS) dan Distributed Denial of Service (DDoS);
b. Ransomware;
c. Malware;
d. Phishing;
e. Spyware; dan
f. Unauthorized Activity.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

DSF-CSIRT akan melakukan kerja sama dan berbagi informasi dengan tim CSIRT/TTIS atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diberikan dan diterima oleh DSF-CSIRT harus dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa DSF-CSIRT 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

5.1. Layanan Utama

5.1.1 Pemberian Peringatan Terkait Keamanan Siber

Memberikan peringatan terkait adanya insiden siber kepada pemilik sistem elektronik melalui email kepada seluruh konstituen DSF.

5.1.2 Penanganan Insiden Siber

Melakukan analisis, mitigasi, dan pemulihan insiden siber serta mengoordinasikan dan mendukung manajemen krisis penanganan insiden.

5.1.3 Pencatatan setiap laporan/aduan yang dilaporkan

Mencatat setiap laporan atau aduan insiden ke dalam tiket insiden untuk selanjutnya dilakukan penanganan insiden siber.

5.1.4 Pemberian Rekomendasi langkah penanganan awal kepada pihak terdampak

Memberikan rekomendasi langkah penanganan awal kepada pihak terdampak melalui koordinasi dengan konstituen terkait.

5.1.5 Pemilahan (triage) Insiden Siber sesuai dengan kriteria yang ditetapkan dalam rangka memprioritaskan Insiden Siber yang akan ditangani.

Melakukan pemilahan (triage) insiden siber berdasarkan tingkat kritikalitas untuk menentukan prioritas penanganan insiden.

5.1.6 Penyelenggaraan koordinasi penanganan Insiden Siber kepada pihak yang berkepentingan

Mengoordinasikan penanganan insiden siber dengan pihak terkait guna memastikan respons insiden berjalan efektif.

5.1.7 Penyelenggaraan fungsi lainnya sesuai kebutuhan

Melaksanakan fungsi lain yang diperlukan untuk mendukung penanganan dan pengelolaan insiden siber, termasuk dokumentasi, pelaporan, evaluasi, dan penyusunan rekomendasi perbaikan.

5.2.Layanan Tambahan

5.2.1. Penanganan Kerawanan Sistem Elektronik

Mengidentifikasi, menganalisis, dan memberikan rekomendasi penanganan terhadap kerawanan pada sistem elektronik DSF yang berpotensi menimbulkan risiko keamanan siber.

5.2.2. Penanganan Artefak Digital

Mengumpulkan, memeriksa, dan menganalisis artefak digital yang berkaitan dengan indikasi maupun kejadian insiden siber pada sistem dan perangkat DSF.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Menyampaikan hasil analisis potensi ancaman siber kepada seluruh konstituen sebagai dasar untuk meningkatkan kewaspadaan dan melakukan langkah mitigasi yang diperlukan.

5.2.4. Pendeteksian Serangan

Mendeteksi dan mengidentifikasi indikasi serangan siber pada sistem elektronik DSF berdasarkan hasil pemantauan log, peringatan (alert), dan informasi dari perangkat keamanan yang digunakan..

5.2.5. Analisis Risiko Keamanan Siber

Mengidentifikasi dan menganalisis risiko keamanan siber pada sistem elektronik DSF serta memberikan rekomendasi pengendalian untuk mengurangi risiko tersebut.

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Memberikan konsultasi, pelatihan, edukasi, dan simulasi (drill) untuk meningkatkan kesiapan konstituen dalam menghadapi insiden siber, termasuk dukungan aspek teknis dan kebijakan.

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Meningkatkan kesadaran dan kepedulian pegawai DSF terhadap keamanan siber melalui pelatihan, edukasi, serta penyampaian informasi mengenai ancaman dan praktik keamanan siber yang baik.

6. **Pelaporan Insiden**

Konstituen DSF melaporkan dugaan insiden keamanan informasi melalui itsupport@dipostar.com atau sistem tiket DSF. Tim IT Support melakukan penyaringan dan klasifikasi laporan. Laporan yang dikategorikan sebagai insiden keamanan informasi akan diteruskan ke dsf.csirt@dipostar.com untuk ditangani oleh DSF-CSIRT. Pelapor wajib melampirkan:

a. Nama pegawai/pelapor.
b. Bukti insiden (foto, screenshot, log file, atau bukti pendukung lainnya).
c. Informasi lain yang diperlukan sesuai ketentuan yang berlaku.

7. **Disclaimer**

a. Seluruh penanganan insiden siber bergantung pada ketersediaan tools dan sumber daya terkait yang dimiliki oleh DSF-CSIRT.
b. Waktu penyelesaian insiden siber bervariasi sesuai dengan kondisi situasional terhadap insiden yang dihadapi.

Jakarta, 30 September 2026

Ketua DSF-CSIRT

Richardus Bayu