RFC 2350 Telin-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 20 Mei 2024.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan pembaharuan dokumen.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://www.telin.net/en/telin-csirt (bahasa Inggris)
https://www.telin.net/id/telin-csirt (bahasa Indonesia)
Dokumen dapat diunduh di :
https://www.telin.net/telin-csirt/rfc2350

1.4. Keaslian Dokumen

Kedua dokumen telah ditanda tangani dengan PGP *Key* milik Telin-CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 Telin-CSIRT;
Versi	: 1.0;
Tanggal Publikasi	: 20 Mei 2024;
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Telin Computer Security Incident Response Team
Disingkat : Telin-CSIRT.

2.2. Alamat

Telkom Landmark Tower, Tower 2, 16th & 17th floor
The Telkom Hub Jl. Jend. Gatot Subroto kav. 52 Jakarta Selatan 12710 - Indonesia.

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

+62 21 2995 2300

2.5. Nomor Fax

N/A

2.6. Telekomunikasi Lain

N/A

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

csirt[at]telin[dot]net

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

File PGP *key* Telin-CSIRT tersedia pada:
https://www.telin.net/telin-csirt/publickey.asc

2.9. Anggota Tim

Ketua Telkom CSIRT adalah VP Information Technology yang menjabat sebagai Koordinator CSIRT, dengan anggota tim meliputi bidang Security Operation Center (SOC), Legal, Regulasi, Komunikasi & Public Relation, IT & Infrastruktur, dan bidang Layanan & Produk.

2.10. Informasi/Data lain

N/A

2.11. Catatan-catatan pada Kontak Telin-CSIRT

Metode yang disarankan untuk menghubungi Telin-CSIRT adalah melalui *e-mail* pada alamat csirt[at]telin[dot]net atau melalui nomor telepon +62 21 2995 2300 siaga selama 24/7.

3. Mengenai Telin-CSIRT

3.1. Visi

Visi Telin-CSIRT adalah :

Menjadi pusat keunggulan dalam keamanan siber, melindungi aset perusahaan dari ancaman siber, serta memastikan kelangsungan operasional dan kepercayaan para *stakeholder*.

3.2. Misi

Misi dari Telin-CSIRT, yaitu :

a. **Proaktif dalam Melindungi:** Secara proaktif mendeteksi, menganalisis, dan merespons insiden keamanan siber dengan cepat dan efektif untuk meminimalkan dampak terhadap operasi perusahaan.

b. **Memperkuat Pertahanan**: Terus memperkuat postur keamanan perusahaan melalui pengumpulan dan analisis intelijen ancaman, penerapan praktik terbaik keamanan, serta peningkatan berkelanjutan terhadap teknologi dan proses keamanan.
c. **Membangun Budaya Keamanan**: Menciptakan budaya kesadaran keamanan siber yang kuat di seluruh perusahaan, melibatkan semua karyawan dalam menjaga keamanan informasi, serta mendorong kolaborasi lintas divisi untuk mencapai standar keamanan tertinggi.
d. **Menjaga Kepercayaan**: Memastikan kepercayaan para *stakeholder* dengan melindungi informasi sensitif, mematuhi peraturan yang berlaku, serta secara transparan mengkomunikasikan upaya dan pencapaian dalam keamanan siber.

3.3. Konstituen

Konstituen Telin-CSIRT meliputi internal Telin.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan Telin-CSIRT bersumber dari anggaran perusahaan.

3.5. Otoritas

Telin-CSIRT memiliki kewenangan atas konstituennya dalam penanganan, mitigasi, investigasi, dan analisis dampak insiden siber di lingkungan perusahaan. Telin-CSIRT dapat berkoordinasi serta bekerja sama dengan pihak lain yang mempunyai kompetensi untuk insiden siber yang tidak dapat ditangani.

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/*Level* Dukungan

Telin-CSIRT melayani penanganan insiden siber dengan jenis sebagai berikut, namun tidak terbatas pada:
a. Web Defacement;
b. DDoS;
c. Malware;
d. Ransomware;
e. Phishing.

Dukungan yang diberikan oleh Telin-CSIRT kepada konstituen dapat bervariasi bergantung pada jenis dan dampak insiden siber.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

Telin-CSIRT akan melakukan kerja sama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh Telkom CSIRT akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi bersifat biasa dapat menggunakan e-mail tanpa enkripsi data khusus (e-mail konvensional) dan telepon. Namun, untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi PGP pada e-mail atau lampiran e-mail.

5. Layanan

5.1. Layanan Utama

Layanan utama dari Telin-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini dilaksanakan oleh Telin-CSIRT berupa peringatan akan adanya ancaman siber kepada pemilik/penyelenggara sistem elektronik.

5.1.2. Penanganan Insiden Siber

Layanan penanganan insiden siber mencakup siklus penuh penanganan insiden. Penanganan dapat dilaksanakan on-site secara langsung atau pemberian saran penanganan untuk ditindaklanjuti.

5.2. Layanan Tambahan

N/A

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt[at]telin[dot]net dengan melampirkan sekurang-kurangnya: file log, timestamp, screenshot, nama pelapor, dan nomor telepon pelapor.

7. *Disclaimer*

7.1 Telin-CSIRT melaksanakan kegiatan tanggap insiden dengan menerapkan prinsip kerahasiaan sebagai prinsip kerja, pembagian informasi ke para pihak akan dilakukan dengan menerapkan prinsip need-to-know.

7.2. Telin-CSIRT hanya menyediakan sarana komunikasi melalui kanal yang tercantum pada RFC2350. Telin-CSIRT tidak bertanggung jawab atas komunikasi yang mengatasnamakan Telin-CSIRT melalui kanal lain.

RFC 2350 Telin-CSIRT

8. Document Information

This document contains a description of Telin-CSIRT based on RFC 2350, namely basic information about Telin-CSIRT, explaining responsibilities, services provided, and how to contact Telin-CSIRT.

8.1. Latest Update

The document is version 1.0, which was published on June 4, 2024.

8.2. List of Distribution for Notifications

There is no distribution list for document update notifications.

8.3. Location to Obtain this Document

This document is available at :
https://www.telin.net/en/telin-csirt (English)
https://www.telin.net/id/telin-csirt (Bahasa)

Document can be downloaded at :
https://www.telin.net/telin-csirt/rfc2350

8.4. Document Authenticity

Both documents have been signed with the PGP Key owned by Telin-CSIRT. For more clarity, refer to Section 2.8.

1.5 Document Identification

Document attribute are :

Tittle	: RFC 2350 Telin-CSIRT;
Version	: 1.0;
Publication Date	: June 4, 2024;
Expiration	: This document is valid until the latest document is published.

9. Data/Contact Information

9.1. Team Name

Telin Computer Security Incident Response Team
Abbreviated : Telin-CSIRT.

9.2. Address

Telkom Landmark Tower, Tower 2, 16th & 17th floor
The Telkom Hub Jl. Jend. Gatot Subroto kav. 52 Jakarta Selatan 12710 - Indonesia.

9.3. Time Zone

Jakarta (GMT+07:00)

9.4. Phone Number

+62 21 2995 2300

9.5. Fax Number

N/A

9.6. Other Telecommunications

N/A

9.7. Electronic Mail Address (*E-mail*)

csirt[at]telin[dot]net

9.8. Public Key and other Encryption Information/Data

PGP key file of Telkom CSIRT available at:
https://www.telin.net/telin-csirt/publickey.asc

9.9. Team Member

VP Information Technology serving as the CSIRT Coordinator, with team members covering Security Operation Center (SOC), Legal, Regulations, Communication & Public Relations, IT & Infrastructure, and Services & Products..

9.10. Other Information/Data

N/A

9.11. Notes on Contacting Telin-CSIRT

The suggested method to contact Telin-CSIRT is via email at csirt[at]telin[dot]net or via the 24/7 standby telephone number +62 21 2995 2300.

10. About Telin-CSIRT

10.1. Vision

The vision of Telin-CSIRT is:
To be a center of excellence in cybersecurity, protecting company assets from cyber threats, and ensuring operational continuity and stakeholder trust.

10.2. Mision

The mission of Telin-CSIRT is:

a. **Proactively Protecting:** Proactively detect, analyze, and respond to cybersecurity incidents quickly and effectively to minimize the impact on company operations.
b. **Strengthening Defense:** Continuously strengthen the company's security posture through the collection and analysis of threat intelligence, the implementation of best security practices, and the continuous improvement of security technology and processes.

c. **Building a Security Culture:** Create a strong cybersecurity awareness culture throughout the company, involve all employees in maintaining information security, and encourage cross-division collaboration to achieve the highest security standards.
d. **Maintaining Trust:** Ensure stakeholder trust by protecting sensitive information, complying with applicable regulations, and transparently communicating cybersecurity efforts and achievements.

10.3. Constituents

Telin-CSIRT constituent include internal Telin.

10.4. Sponsorship and/or Affiliation

Funding for Telin-CSIRT comes from the company's budget.

10.5. Authority

Telin-CSIRT has authority over its constituents in handling, mitigating, investigating, and analyzing the impact of cyber incidents within the company environment. Telin-CSIRT can coordinate and collaborate with other parties with competence in handling unmanageable cyber incidents.

11. Policies

11.1. Types of Incidents and Support Levels

Telin-CSIRT serves to handle cyber incidents of types including but not limited to:
a. Web Defacement;
b. DDoS;
c. Malware;
d. Ransomware;
e. Phishing.

The support provided by Telin-CSIRT to constituents may vary depending on the type and impact of cyber incidents.

11.2. Collaboration, Interaction, and Information/Data Disclosure

Telin-CSIRT akan melakukan kerja sama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh Telkom CSIRT akan dirahasiakan.

11.3. Communication and Authentication

For regular communication, conventional email without special data encryption (conventional email) and telephone can be used. However, for communications containing sensitive/limited/confidential information, PGP encryption can be used for email or email attachments.

12. Services

12.1. Primary Service

The primary services of Telin-CSIRT are :

12.1.1. Provision of Cybersecurity Alerts

This service is provided by Telin-CSIRT in the form of alerts about cyber threats to the owners/operators of electronic systems.

12.1.2. Cyber Incident Handling

Cyber incident handling services encompass the full cycle of incident handling. Handling can be done on-site directly or advice on handling can be provided for follow-up.

12.2. Additional Service

N/A

13. Incident Reporting

Reports of cybersecurity incidents can be sent to csirt[at]telin[dot]net, attaching at least: log files, timestamps, screenshots, reporter's name, and reporter's telephone number.

14. Disclaimer

7.1 Telin-CSIRT conducts incident response activities applying confidentiality as a working principle, information sharing with parties will be done applying the need-to-know principle.

7.2. Telin-CSIRT only provides communication channels listed in RFC2350. Telin-CSIRT is not responsible for communications impersonating Telin-CSIRT through other channels.