

RFC 2350 LamTim-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1 yang diterbitkan pada tanggal 22 Agustus 2024.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan mengenai pembaharuan dokumen.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
<https://lamtim-csirt.lampungtimurkab.go.id/docs>
(versi Bahasa Indonesia)

1.4. Keaslian Dokumen

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

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 LamTim-CSIRT;
Versi : 1;
Tanggal Publikasi : 28 Agustus 2024;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan

2. Informasi Data/Kontak

2.1. Nama Tim

Tim Reaksi Insiden Keamanan Komputer (*Computer Security Incident Response Team*) Kabupaten Lampung Timur.
Disingkat : LamTim-CSIRT.

2.2. Alamat

Dinas Komunikasi dan Informatika Kabupaten Lampung Timur
Jl. Buay Anak Tuha Komplek Perkantoran Pemda, Sukadana
Lampung Timur, Indonesia

2.3. Zona Waktu

Kota Sukadana (GMT+07:00)

2.4. Nomor Telepon

(+62) 858 4081 4097

2.5. Nomor Fax

Tidak Ada

2.6. Telekomunikasi Lain

Tidak ada

2.7. Alamat Surat Elektronik (E-mail)

csirt@lampungtimurkab.go.id

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

Bits : 3072-bit RSA (secret key available)
ID : LamTim-CSIRT <csirt@lampungtimurkab.go.id>
Key Fingerprint : Ulun1keyD9BM6231W36gcTKGQOEbcHKKcnwlpoq+gs0

-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: User-ID: LamTim-CSIRT <csirt@lampungtimurkab.go.id>
Comment: Created: 27/08/2024 06:00
Comment: Expires: 07/08/2027 12:00
Comment: Type: 3072-bit RSA (secret key available)
Comment: Usage: Signing, Encryption, Certifying User-IDs
Comment: Fingerprint: 7D0F73D0D3EBA5411CC60DECE6032B3103544405

mQGNBGB0YwkBDADMRDEHhLU897pDsgOMmAHR5VAERUoNNMHUZtDV2verLOl69ea7
FYrZYZXiHKG3IrhDIJZIX2Ja3HL7k4RHyZFQ0B0J4+HsOIBiT7n9Qio7dHeSJOCKg
n++HAXLGimx5Idfpy6vzjhEcflshzJSOIqNre3jqox61qVmpIUtWQheHpPPYDvr
5f89Jlp16BOQ5waUdoZ64NMvmVp6MCJIy6lxgzkS0jM16nIddJqeRpQ2QezwSe1
F8FEED06zK06XADzBG2eNSXPN8SXEGrlyr4944PjCRoNNyy4mlAuTutDAIbwt2n
sNyCLN0SQ/Wd3x91c7PPrlIyOTw8YLoq+hWvuPCNaprxpLJIgYAS1XY49IEWvtT
YYz4UKNlb950624dQr9eTdZVZyLBxHLsdWilx2pJCyE+l0anDDcCG0K2JylfTYS5
4ONcqHXXZeki76R8BqjJhl5YUYxq2HdMqf41CTFRnSvwZAIWqbdKQMDnbGUeED2I
jB0Omww6efZZIY8AEQEAAABQqTGFtVGltLUNTSVJUIDxjc2lydEBsYW1wdW5ndGlt
dXJrYWluZ28uaWQ+iQHUBBMBCgA+FiEEpfVdJWq4WhDRtl1gdq6OrMfk0dMFAmbO
YwkCGwMFCQPCZwAFCwkIBwIGFQoJCA5CBBYCAwECHgECF4AACgkQDq6OrMfk0dMc
BAv+KRfj8m5sCyMtn57YBc4ZvOzl/3tr+SPG1TRt7J4mClowGa6Xr0g5ymkKBE7W
FOdzQKVVR0fAG1Y7jydM1UQh2bF6JyViQHWDV5Qv//Hx0yF14uU16xyxtzcpLBJ0
+ZzQxmj3/6WjvucPlor7f3xk9dmG2AIWWDw5FhFLR6txCewX55KUSMR+QVlmF1P5
3dfk9eQXJMJ1v0VmfKJLGTTGyiDD360ZyVkmIyvBrFflORivu1ik4viFOH8pcNI
CyHxf1naDGtNyAEw8xb2M6fkn4IeE1HNCO9WsBHMNp4IZm8vo7gQ0FesYXv2QSNj
GEqHV9vmq3wyVbkvuCHSgWQwqjx2wAiEKz1SAsaduT7UgmflKyYx8qKtvx2FDJlW
z4Tyszm+TZfJ9IIZn1Kj3Xc54ua1IhuBMc7svvhoinlWeaVvCoLcNMNPUVhI2h1Y
PNVnYx+vN78Rg186kJiNHMYEYtY6SoEOXrHfD+hfmUJRuOeLo0LM4+kmbFGvGu0m
vUzGuQGNBGB0YwkBDADKiFp5FtDK+QVtgvBVJa/FRjnfKdYml1+0sI96BQycdtlt
tU7aI8ehDRyNwX+ZoSAzq8tQWxmguVWun7Z+tisu8yKXu4GmXzkbbrbxcmRIJ/4
ooRiHK853aQyEd1RKOS4EbnhSNnlQyUkqBz3NGf47DN9P8r/zzV+5T6rW4yC/4sg
4EfZ09PHBSLQVB2nH2ALG17gRwt09q4FRr6PcsD86mbJHig6SkNqm4aNJ/OjHhZ
bVpAgym2yGcG4szedG5B2N3PEyxl0E9+OnDZs16zVW3oIUUpTrMGzxN0xE+7FyrK/
+LekIZ2Hjg14xbqSSo+cuC75h7oxpkhFr8aaWW9PuMXv8XNmrFyXYn9NnCSCEtoD
3csHBuly+ISuum8J58Dif6EIT3P6DETTWr1qqLaDBdo9bPNYCWa3zGNq5IiHoisF
3vAP14QES+dHRbM6FVJUWoKV8S3T7xdTAyw2tbyCDL5whTtf7MIEdDbGFaAEVGBW
DizRj7AX2EVE1XznEx0AEQEAAAYkBvAQYAQoAJhYhBKX1XSVquFoQ0bZdYHaujzH
5NHTBQJmzmMJAhSMBQkDwmcAAAOJEHaujzH5NHTFjAL/Rq4qW1mEHdfIgv0RFy
e+zOzLZTWLbQQL9009yBXpq50d0WRHvUVfKe1ryJGBUKyczif5nYayvGFTWJ/Uge
snS2mI+YEqxL3lp/rZv+EvHD59Ni8dKdrG7oxBN7sMZjgrykTzG2hLJsC0OCkEg
TCqu/HYO3ybsprw9ahavCri3y6ficKJeV8mPDxr/9h2EW5Y1Jr96kaj98yJPETgm
wDwTYKEQYAQelaki+1srD4IzxXss938WdyN5/0Gbq6C7jZvx1uDpG9WQjYEcvX2q
ixlkhpg5XG/bwJQDB1z/r49JDh7J0clIRDop/24iyUxuuGwEq5xzQa+RkgzdOmrD
on8DAV3aywGeb0xf7BsqkusQUaF0C0F+sg7h+MMX2aGbJiQ9aJQOr/rIwVbLgRO+
CYbqgwHrhilHnU1h8xYnI3wY3Y1k95S0vMiy6+NMIg78wdCy6s4etiedUuSyx7ag
awVmvSrMGXvpM3opJuzLUexhXm48I9MQgLXK3/QWyh28Dw==
=dCTe
-----END PGP PUBLIC KEY BLOCK-----

File PGP key ini tersedia pada :

<https://lamtim-csirt.lampungtimurkab.go.id/docs>

2.9. Anggota Tim

Ketua LamTim-CSIRT adalah Kepala Dinas Komunikasi dan Informatika Kabupaten Lampung Timur, Sekretariat CSIRT adalah Sekretaris Dinas Komunikasi dan Informatika Kabupaten Lampung Timur. Yang termasuk anggota tim adalah Tim Reaksi Insiden Keamanan Komputer (*Computer Security Incident Response Team*) Kabupaten Lampung Timur.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak LamTim-CSIRT

Metode yang disarankan untuk menghubungi LamTim-CSIRT adalah melalui *e-mail* pada alamat `csirt[at]lampungtimurkab[dot]go[dot]id` atau melalui nomor telepon (+62) 858 4081 4097

ke Bidang Persandian dan Statistik Dinas Komunikasi dan Informatika Kabupaten Lampung Timur pada hari kerja.

3. Mengenai LamTim-CSIRT

3.1. Visi

Visi LamTim-CSIRT adalah “Menjadi garda terdepan dalam melindungi aset informasi dan infrastruktur teknologi dari ancaman siber melalui respons insiden yang cepat, tepat, dan proaktif, serta meningkatkan keamanan digital secara keseluruhan”.

3.2. Misi

Misi dari LamTim-CSIRT, yaitu :

1. **Mencegah dan Mengurangi Dampak Insiden:** Meningkatkan kewaspadaan terhadap ancaman siber dengan proaktif dalam mendeteksi dan mencegah insiden keamanan sebelum terjadi, serta meminimalkan dampak insiden yang sudah terjadi.
2. **Respon Cepat dan Efektif:** Menyediakan layanan respons insiden yang cepat dan efisien untuk mengatasi ancaman siber, serta memulihkan sistem dan data dengan cepat setelah terjadi insiden.
3. **Peningkatan Kesadaran dan Kapasitas Keamanan:** Memberikan pelatihan dan sosialisasi kepada seluruh pemangku kepentingan mengenai pentingnya keamanan siber dan langkah-langkah pencegahan yang dapat dilakukan.
4. **Kolaborasi dan Koordinasi:** Bekerja sama dengan tim keamanan lain, baik di dalam maupun luar organisasi, untuk berbagi informasi dan strategi dalam menangani insiden keamanan siber secara efektif.
5. **Pengembangan Kebijakan dan Prosedur Keamanan:** Merumuskan dan mengimplementasikan kebijakan serta prosedur keamanan yang berkelanjutan untuk memastikan perlindungan optimal terhadap aset informasi dan infrastruktur teknologi.

3.3. Konstituen

Konstituen LamTim-CSIRT meliputi Perangkat Daerah di lingkungan Pemerintah Kabupaten Lampung Timur.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan LamTim-CSIRT bersumber dari APBD Dinas Komunikasi dan Informatika Kabupaten Lampung Timur.

3.5. Otoritas

LamTim-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber di lingkungan Pemerintah Daerah Kabupaten Lampung Timur.

LamTim-CSIRT melakukan penanggulangan dan pemulihan atas permintaan dari konstituennya dan dapat berkoordinasi dengan BSSN / Pihak lainnya untuk insiden yang tidak dapat ditangani.

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/Level Dukungan

LamTim-CSIRT melayani penanganan insiden siber dengan jenis berikut :

- a. Web Defacement;
- b. DDOS;
- c. Phising.

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

LamTim-CSIRT akan melakukan kerjasama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber.

Seluruh informasi yang diterima akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa LamTim-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 Reaktif

Layanan reaktif dari LamTim-CSIRT yaitu :

5.1.1. Pemberian Peringatan Siber

Layanan ini berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik.

5.1.2. Penanggulangan dan Pemulihan Insiden Siber

Layanan ini berupa koordinasi, analisis, rekomendasi teknis, dan bantuan on-site dalam rangka penanggulangan dan pemulihan insiden siber.

5.2. Layanan Proaktif

Layanan proaktif dari LamTim-CSIRT yaitu :

5.2.1. Penilaian Keamanan (*security assessment*)

Layanan ini berupa identifikasi kerentanan dan penilaian risiko atas kerentanan yang ditemukan.

5.3. Layanan Manajemen Kualitas Keamanan

Layanan manajemen kualitas keamanan dari LamTim-CSIRT yaitu :

5.3.1. Edukasi dan Pelatihan

Layanan ini berupa pembangunan kesadaran dan kepedulian terhadap keamanan siber dengan melaksanakan edukasi dan pelatihan.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke [csirt\[at\]lampungtimurkab\[dot\]go\[dot\]id](mailto:csirt@lampungtimurkab.go.id) dengan melampirkan sekurang-kurangnya :

- a. Foto/*scan* kartu identitas
- b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan

7. Disclaimer

Tidak ada.