

RFC 2350 MAKASSAR-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 15 Februari 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 :
csirt.makassarkota.go.id/file

Keaslian Dokumen

Kedua dokumen telah ditanda tangani dengan PGP Key milik Bidang Persandian Dinas Komunikasi dan Informatika Kota Makassar. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 MAKASSAR-CSIRT;

Versi : 1.0;

Tanggal Publikasi : 15 Februari 2024;

Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

MAKASSAR - Computer Security Incident Response Team (CSIRT) Indonesia
Disingkat : Makassar-CSIRT Indonesia

2.2. Alamat

Dinas Komunikasi dan Informatika Kota Makassar
Jl. A. P. Pettarani No.62, Tamamaung
Kec. Panakkukang
Kota Makassar
Sulawesi Selatan 90232

2.3. Zona Waktu

Makassar (GMT+08:00)

2.4. Nomor Telepon

Telepon (0411) 4671729
Telepon 112

2.5. Nomor Fax

(0411) 4671729

2.6. Telekomunikasi Lain

Tidak ada

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

csirt[at]makassarkota.go.id

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

-----BEGIN PGP PUBLIC KEY BLOCK-----

```
xsDNBGYLf2IBDACfRLSXqjH7z2h8hiGHtOlg+rhUm/dHOnIOCrtjrGFQD5a7rcAj
H/gQ1+7Owvc4SaWSOFXs0dfx4L9daSWPPGpJsJkEKasv3tlcx45Z/mp4Q81eu4C4
Da5fJo29HZLYqXfypYliC5L6860RZkttRB+WYY/4NQpRdWgxK4GrCaQL+itlgr2l
N9u5C5Q91CTupssJSKC+MLheSfoAH/hwR5Kp627IDg4pmXU72/rZLFo+xTpaUoHP
RyftQ9Sb0fZCUY1EIOHaQf40GyC9LIQIHjha7KAwZJxPWzbSmTYOMFm8GT/dSldN
cBW7xp2fzpguDWZBIQngXK+LsBo1VM5/LNMWYjrSzRES6dvoqJYy+tssTav4LkGK
d2dZzmlQJOvUOXs44cYfSg7zyrjOrbA/k6CNvFb27gIHvOMldgfDVOYMHRMh5xUM
5jaa596iNoanbONF6VmoyfWCQmhr19asS3COemnjhEWiLMMdPufapG4DJaM3koDK
rab6Ur4kv8oeVvsAEQEAAc0zY3NpcnRABWFrYXNzYXJrb3RhLmdvLmlkIDxjc2ly
dEBtYWthc3NhcmtvdGEuZ28uaWQ+wsENBBMBCAA3FiEE5xweqqYtKS//nHwtaQmp
Eu/s2bQFAMyL2f2FCQImAYACGwMECwklBwUVCAkKCwUWAgMBAAAKCRBpCakS7+zZ
tlqgDACIfjF5B/rrblE9Kae8drCTddS759XvaD/UDnfHJaUW35zc3Aqr2GPjHjPQ
AnnI9pIy2hHD75vcqfI6znaaw6dW56XXK7zx1R5n/GHOhep/YH2DnN+V0dxDUeIH
yVxwXRnBvb6XMURzuJgXMfeY2zTbjDGo48haQy1n6j9bWwNupC/Znk1Lm/9Ct+aX
j8H/xZwflHROAWAKrNuxWoGHYQ5J1iEchrO1n7IGNNwksFAvd1ayMuUXLUBHHeFA
UxgYEzSrC/Rst8XtLe15iO5mAY3ulp+OJzV/PpflEaDWJabaYVfW3hO+266qhyF1y
LxZbb92EHQeK15o2ieW/KqltpsH/6yWIAftUMgWdF3lqJINDatOJGSsjyq5Guk0M
c4xlyfSNuqEx57UN99xi5ataqFu96lhvlagxRPKgtVS4Kdm46MNwvj4zjMzLF186
NGYPV+hGcWPCFOyPS3FE5iWY6JrunNP2tGZg3Rlac6meUwiNMHgbtGZXXZgWta
BL990G3OwM0EZgt/YwEMAK5GflLyTP8UmqlCaNuG42sL7EERFr2Vpezl7W1qn+tN
1Lud3FBLcN98MNzNdh4/mMNOH8vMN3yCh01TyZpsOleZQhPHrzanh1Kf8foOfGcM
1pvm8i31Pa/FEohQyp458sBYyW8gpnQov4k7qex9QXYzS4CF1t2h3NLvwNS8Dq8z
b+HO6gcGk6dkvU5PFhQcD1Wiv3RgBxS6l4h/5SSj8+UwW2pNjmgKRN7COiGJN5Lp
98nmD5ieo84qq+eNtitF3n0MKIXyDXRvoTbLolag+8PmMQ5p9z8Go6/PkF9tDxKT
k5KqxJZb5GROoiZ0BPWUdWPxZpZz7tDiXA53W/+9P5Sa6E2zbfzbxexTBLicWe3P
1JcA4PJAYyaB7RnrIPtkF+HhHT/cobs/4UIQ9IH8O1P8ID3QMoREKfCajNAipCIR
2JsNI5ZNcm9ZNCqjadv9UtN3liP21hEEWO43hStn/X07xKMk12vKN720kQd0zj+t
kr9Re52QxIP5YIFDIA9d3wARAQABwsD8BBgBCAAmFiEE5xweqqYtKS//nHwtaQmp
Eu/s2bQFAMyL2f2MFCQImAYACGwwACgkQaQmpEu/s2bSqDAv/dGg4yLpYUlxdaaly
wBQmXeZBu1EGFHDkMLipjO/Fyf2pDC3iy1MzEk2jfgd/vB7piqZgKZPO4vX4wrhH
0Tnn2kAzN47DjgEQ8bCjFI0pKHdTzDENS2JAW0D5RuwRsqvGkA6DfnWXpaaEPfp
9HPbabvJ622RqnvOIL9bsObnzseT10VC3w1dS52xqCeeuY+Pkz6xjhujV/b1Dqkg
JZW+lrsUknn1bSPhe6hqtBjxTWZ8+LtlAyrEhRCPsog6zflueX4J5rxPGjcwGU
k6d0Z1PZywOi7VOGNQx52fpDHNn+IAKYjb4P4Z2rRqrPRrVba120V/7bs0E0ayqm
ADxiU8VI6Q7ho9CUBWdiNh/hpmVhsGK+JO2O4WON7I0jzd8HFFVjKuhH9c3CHs+BV
rzYx16VezfEmc7Xkhi0ed7bFsc9MSLDKI0HM4G4R+s2QBO9fOIfDrmNzThY324F8
1YKUMYwk3Qik9zs2iAnkrScb9JDs54PZKyW6ee7bfcQdGIIC
=ERI6
```

-----END PGP PUBLIC KEY BLOCK-----

File PGP key ini tersedia pada :

csirt.makassarkota.go.id/pgp

2.9. Anggota Tim

Ketua Makassar-CSIRT adalah Kepala Dinas Komunikasi dan Informatika Kota Makassar. Yang termasuk anggota tim adalah seluruh staf Bidang Persandian dan Bidang Aplikasi dan Telematika serta Pegawai lainnya yang telah disebutkan dalam SK Walikota Makassar tentang Pembentukan Tim CSIRT Pemerintah Kota Makassar.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak Makassar-CSIRT

Metode yang disarankan untuk menghubungi Makassar-CSIRT adalah melalui *e-mail* pada alamat csirt[at]makassarkota[dot]go[dot]id atau melalui nomor telepon (0411) 4671729 dan 112 ke Dinas Kominfo Kota Makassar pada hari dan jam kerja senin s.d jum'at pukul 07.30 s.d 15.30 wita. Adapun selain pada hari dan jam kerja tersebut akan dilakukan pada hari dan jam kerja selanjutnya atau pada hari yang sama berdasarkan tingkat kedaruratan insiden siber.

3. Mengenai Makassar-CSIRT

3.1. Visi

"Menjadi pilar utama keamanan siber Pemerintah Kota Makassar yang inovatif dan proaktif, melindungi infrastruktur digital, serta membangun ekosistem teknologi yang aman untuk mendukung pertumbuhan dan kesejahteraan masyarakat."

3.2. Misi

Misi dari Makassar-CSIRT, yaitu :

a. Deteksi dan Respons Cepat:

Mengembangkan kemampuan deteksi dini terhadap ancaman keamanan siber dan merespons insiden dengan cepat untuk meminimalkan dampak negatif.

b. Peningkatan Kesadaran Keamanan:

Menedukasi dan meningkatkan kesadaran keamanan siber di kalangan pegawai pemerintah, masyarakat, dan pemangku kepentingan lainnya.

c. Kolaborasi Antar instansi:

Berkoordinasi secara efektif dengan instansi pemerintah pusat bidang siber, dan lembaga keamanan siber lainnya untuk meningkatkan pertukaran informasi dan respons terhadap ancaman berskala besar.

3.3. Konstituen

Konstituen Makassar-CSIRT meliputi Organisasi Pemerintah Daerah (OPD) dilingkungan Pemerintah Kota Makassar termasuk perangkat kecamatan.

3.4.Sponsorship dan/atau Afiliasi

Pendanaan Makassar-CSIRT bersumber dari Anggaran Pendapatan dan Belanja Daerah Kota Makassar

3.5. Otoritas

Makassar-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan insiden keamanan siber pada Pemerintahan Kota Makassar. MAKASSAR-CSIRT melakukan penanggulangan dan pemulihan atas permintaan dari konstituennya.

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/Level Dukungan

Makassar-CSIRT menangani insiden yaitu :

- a. Web Defacement;
- b. Distributed Denial Of Service (DDOS);
- c. Malware;
- d. Web shell
- e. Spam SEO

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

Makassar-CSIRT akan melakukan kerjasama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh Makassar-CSIRT akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa Makassar-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

Layanan utama dari Makassar-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini dilaksanakan oleh Makassar-CSIRT berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik dan informasi statistik terkait layanan ini diberikan oleh Makassar-CSIRT

5.1.2. Penanganan Insiden Siber

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

5.2. Layanan Tambahan

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini diberikan oleh Makassar-CSIRT berupa koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan (hardening), layanan ini hanya berlaku apabila syarat- syarat berikut terpenuhi :

- a. Pelapor atas kerawanan adalah pemilik sistem elektronik. Jika pelapor adalah bukan pemilik sistem, maka laporan kerawanannya tidak dapat ditangani;
- b. Layanan penanganan kerawanan yang dimaksud dapat juga merupakan tindak lanjut atas kegiatan *Vulnerability Assessment*.

5.2.2. Penanganan Artefak Digital

Layanan ini diberikan oleh Makassar-CSIRT berupa penanganan artefak dalam rangka pemulihan sistem elektronik terdampak ataupun dukungan investigasi. Makassar-CSIRT memberikan informasi statistik terkait layanan ini.

5.2.3. Audit dan Penilaian Keamanan

Layanan ini diberikan oleh Makassar-CSIRT berupa audit dan penilaian keamanan sistem elektronik.

5.2.4. Edukasi dan Pelatihan

Layanan ini dilaksanakan oleh Makassar-CSIRT berupa Edukasi dan Pelatihan Keamanan Siber kepada anggota Makassar-CSIRT dan Agen Siber.

5.2.5. Pembangunan kesadaran dan kepedulian terhadap keamanan siber

Layanan tambahan Makassar-CSIRT secara aktif membangun kesiapan instansi pemerintah dalam melakukan penguatan, penanggulangan dan pemulihan insiden keamanan siber melalui kegiatan literasi dan bimbingan teknis.

6. Pelaporan Insiden

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

- a. Foto/*scan* kartu identitas
- b. Bukti insiden berupa foto atau *screenshot* atau *log file* yang ditemukan
- c. Atau sesuai dengan ketentuan lain yang berlaku.

7. Disclaimer

Penanganan Insiden Malware bergantung pada ketersediaan sumber daya yang dimiliki.

Makassar, 10 Juni 2024

Plt. Kepala Dinas Kominfo
Kota Makassar



Isnawaty Nur, ST., M.Sc., Ph.D
Pangkat Pembina TK I
NIP. 19740607 200411 2 001