RFC 2350 SUBANG-CSIRT

1. Informasi Mengenai Dokumen

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

   1.1 Tanggal *Update* Terakhir

   Dokumen merupakan dokumen versi 1.1 yang diterbitkan pada tanggal 16 November 2022.

   1.2 Daftar Distribusi untuk Pemberitahuan

   Menjabarkan pihak-pihak yang menjadi daftar distribusi untuk pemberitahuan RFC 2350, disesuaikan dengan kebutuhan masing-masing CSIRT.

   1.3 Lokasi dimana Dokumen ini bisa didapat

   Dokumen ini tersedia pada :

   http://csirt.subang.go.id/rfc2350/rfc2350-id.pdf (versi Bahasa Indonesia)

   1.4 Keaslian Dokumen

   Kedua dokumen telah ditanda tangani dengan PGP Key milik Bidang Teknologi Informasi Komunikasi dan Persandian, Dinas Komunikasi dan Informatika Kabupaten Subang. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

   1.5 Identifikasi Dokumen

   Dokumen memiliki atribut, yaitu :

Judul	:	RFC 2350 Subang-CSIRT;
Versi	:	1.1;
Tanggal Publikasi	:	16 November 2022;
Kedaluwarsa	:	Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

   2.1 Nama Tim

   Tim Tanggap Insiden Keamanan Siber Pemerintah Daerah Kabupaten Subang / *Computer Security Incident Response Team* Kabupaten Subang

   Disingkat : Subang-CSIRT

   2.2 Alamat

   Jalan Mayjen Sutoyo No. 46, Kelurahan Karanganyar, Subang – Jawa Barat

   2.3 Zona Waktu

   Waktu Indonesia Bagian Barat (WIB)

   2.4 Nomor Telepon

   (0260) 411318

   2.5 Nomor Fax

(0260) 411318

2.6 Telekomunikasi lain

Tidak Ada

2.7 Alamat Surat Elektronik (E-mail)

csirt[at]subang[dot]go[dot]id

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

Bits : 4096 bit

ID : Subang-CSIRT (csirt[at]subang.go.id)Key

Key Fingerprint : 4CB7D2774BD0AB5A493FACF2B8A676E69E069690

-----BEGIN PGP PUBLIC KEY BLOCK-----
mQINBGMamNcBEAC7ro3Lxbx59Uz8Npu/akydDVp+r064EtTz0Ai6P/0q9Qkt7t16
j28GMQZP4SC7e4cj0f3uuZMUjdNG2rgeWdFcE1Khab9k2UKn+tqJEGoqxyEb0hiF
oFqtDY0exL7ancK63wJzmGwdSn+Y1jqRQpoY/yrrTl4HFILf3g8Yc3BSTGq+dyOR
OhVRkl/a+2QUCZFBx7CFp84MX2uyItnomlXTbtbjQ1b40XZXuvOqLFmRHY9kTTF1
Gf7n8Ycsoe5Ui1kIFbo7jNo05kBtNWZ1eEIfbISw6UxFJD/LoPP1GypJS1y/U0sv
aaHGothW32ev46RGclQf7jtVY8AbpaXR3OzxcFhHF1XaaIKwE65nKZKNIRZ5hUN/
tZFBuGeb5Us568IMv3fb3zEGEjxKyGCUFHyQafi5Sbc/449Z6ZA+cssuv7diA5HS
5ZIyEl8Zpwl3ULCqsvvY4a8XRTIGIDM7sBZ52P+3O3PYoW2U1JrmpKODLB7XlJ3T
yQXmwRrFgNlNflTwV0zxJmgy6K1OW3ias/0Eo+Q8Z2iichI+whv1HaVxnhgD9YdL
WM+xj+RPzI4eqWgcUfCTGwMR0JV/FycuUXFV3tBvtwJrVNx1tUFttk+hAhPttiM2
MwufYVDit2KyIw+BQuEG/+85KOk0SG0hKWDWW8FQbRwhtwM6V8WWbpCiuQARAQAB
tCFTdWJhbmctQ1NJUlQgPGNzaXJ0QHN1YmFuZy5nby5pZD6JAlcEEwEIAEEWIQRM
t9J3S9CrWkk/rPK4pnbmngaWkAUCYxqY1wIbAwUJA8Pn+QULCQgHAgIiAgYVCgkI
CwIEFgIDAQIeBwIXgAAKCRC4pnbmngaWkCVCD/49T2KIq6Fo9BLZfr1OrBXiTOM1
4mf9cJBF/8ca3W7p/ZbdFf14xDy1vHEU+TcQYL6Ka/K8MOGd7iJc7LgZ4lMIkxT8
Lc+fWSLu6LPUF+Q+OZ+EuH8P1OJ75zSJ1Mzaufnv+uZhycy5nWtCNPn29KZWneLW
9VSlW4tjfazFhiGJqoLNibRUshQpK5nwGckZ8BRZkqcz/Cp5eR6iuT1S/1rjbT2V
kZW9vXbT9vsypiKGz47a/kyjWmsxy/UAd54hK95PKPQ0axlaLyoXEvfV8GJzINzb
DA+wNsQgUnk8o7ia5AJGg+aJK7AE5YdwM0SZZyEJJaL1HQPdZ4S0U5r8KQh2oLj3
E4JHiRM5SVi2qCEmAoe4z3WnF7X4sGktVOFqphlq2oq1ctKO0FYeqap6WjnLpMo2
eTDccLSMf/ZwoDrfrNHGT0rjF93HktMWpZz/I4xH6OGvYzKpCPwu2HFQBNGuil1v
enHJKE2MksQ+5w3/V9OtNCJ/nZcbBe92PChWrBpR7gba4y7KW2SnjdRX0ReiXuu5
Ev4VRtJsv2UxkZkfPjV9TeVaA+buVG2mP86NSqSZgdqJ047BiZRhjQ+nbLDCuPeH
UJyft5N06pvqMkQ3YH2cP8CPhCByby4mo2IBqr7FXsWtsHBOI2BgXtjoGjWU+mjh
LJTZ7Zr6LLwKChOm87kCDQRjGpjXARAAvv5UHn+voXnIkjA0ivqzWv/ca6AWfnj/
cnHqX7UmLTB8PjRaxmFSnYI7e+R5JlSOuCMgM2D4kGAhuac7wRHbK/z63Ns2fbJI
UYMZJFl0O1ozfx/UKxq9bNNmUT1fNpJvbz8yHx1OVpqxJXQzM74NxS/TaE1S1ZuE
Vuj+tYdtiEkk/ehzxBpBpHg3I5htdTeAuw5KSrEsmQMviN0uf37qeoq74lAfRhrN
lop5lCBIA1k2Qbkc4QEWZfcMkirMZOzCJ9oCmp9GC8w83iVoscwEB0KiVTHU2E+W
z4+f55SvTi6MNB4T5h5snwmCkxBVb5mN0mjolPSbZQ7MtHT3zh3W2QUNFgUhCuqC
GlMZeDqt57ThBmTuO2iMp65Ld+gX2LR8Y9l6XdbEPZjBSg2oD++RiC16dyiLBIpZ
GjIEFUVa/Zd7Ri+r8eDHEdruMFlwhGrv8hwa5SG/f+A0ISBs16P6fgM0fHASusKw
Rn0YapsYToJquTryd904NZBLJReAbuGkvD0tQ56KBxwcS5I52A1gppPG3bAhN/y1
+ZZlaA7wiZoXyaNjYNdH7Tlj99Vwx3+p8PPTJmW03swGx8GjmzP77mtexCr3KXr2
svJyA2IUbj0BTDDcl4T0++CU8XwkG2lsWFxX1LoNZqiBgOJjX8po3iQjn+YZ4ndp
rKwbgR57YMUAEQEAAYkCPAQYAQgAJhYhBEy30ndL0KtaST+s8rimduaeBpaQBQJj
GpjXAhsMBQkDw+f5AAoJELimduaeBpaQe8IQAJYy7o4hSIMy087VIT5zT3P1LidP
tUVGnzpqRHekRJW+bqwtyFWpLjI56cCwZhAg+nok6hH3fAJF1O/10s30cRhHgW9C
cKjfER6bICzTryRoeb4VGDjDMQ7nZXWP+N3Q8PfrbLrcK3kQwmSKEqQMAuoYLQd6
1SHj1lcBdMCMlOuARz3C4f1/H7NdamZKGEHYZJPca70YcK81q/ymxiTqi7oKal0V
8/KVWDZnaYFyM+f20pyF+9Zb4NHDyJb12qwLOmcY9xhznjN9jr0fL2oVToktxiQR
7ueZiWbMSffIDg9aVQI2W1Jb9lRDYnjB9ySUuIyqVpiUBq6jFLsKZDUY2lMQRgYt

UQkeyZ+GdBQ0VJ9v66pYrSERfryYA6PorwBM1iHEzEFU/+yAPwqCkgWypTbbFZnx
CMblwGKQudTsyBsA/98Q6HwJt22eIlA9y8MfCutL1dgCGT+mSHVrsW5saMEgzm82
fvm/Jsizhyyzapqj7f2RDWSepsp+7lcWXkmzOeuwseEQL/JbnfGyN1vteBBaeyR+
OnZvWEBl0PWkqtFDdwQLtSaUlRxjTUqZ9fvY5ZZ6rZb6sBMEANnW4ZwloPiBv2wt
vFVt7sQWb6bIrE+n1uobihOuo5LnKTJX6KJ3ZvdhObq3dsCbHwtEbYk5KY5SbGkI
SiUg83OGU4/3WLeD
=/xz/
-----END PGP PUBLIC KEY BLOCK-----

File PGP key ini tersedia pada :

http://csirt.subang.go.id/storage/public-key/publickey.asc

2.9 Anggota Tim

Ketua Subang-CSIRT adalah Kepala Dinas Komunikasi dan Informatika Kabupaten Subang. Yang termasuk anggota tim adalah seluruh staf Dinas Komunikasi dan Informatika dan Organisasi Perangkat Daerah Kabupaten Subang.

2.10 Informasi/Data lain

Tidak Ada.

2.11 Catatan-catatan pada Kontak Subang-CSIRT

Metode yang disarankan untuk menghubungi SUBANG-CSIRT adalah melalui e-mail pada alamat csirt[at]subang[dot]go[dot]id atau melalui nomor telepon (0260) 411318 ke Bidang Teknologi Informasi Komunikasi dan Persandian pada hari kerja jam 08.00 – 15.00 pada hari kerja.

3. Mengenai Subang-CSIRT

3.1 Visi

terwujudnya pengelolaan keamanan informasi di lingkungan Pemerintah Daerah Kabupaten Subang sesuai dengan prinsip keamanan informasi yaitu untuk menjamin ketersediaan (availability), keutuhan (integrity), dan kerahasiaan (confidentiality) Aset Informasi.

3.2 Misi

Misi dari Subang-CSIRT, yaitu :

a. mendorong kegiatan pengamanan informasi dan pencegahan insiden keamanan informasi.
b. membangun kesadaran keamanan informasi pada sumber daya manusia di Lingkungan Pemerintah Daerah Kabupaten Subang.
c. menjamin keamanan informasi aset informasi Pemerintah Daerah Kabupaten Subang.

3.3 Konstituen

Konstituen Subang-CSIRT meliputi Perangkat Daerah di Lingkungan Pemerintah Daerah Kabupaten Subang

3.4 Sponsorship dan/atau Afiliasi

Subang-CSIRT merupakan bagian dari Pemerintah Daerah Kabupaten Subang sehingga seluruh pembiayaan bersumber dari APBD Kabupaten Subang.

3.5 Otoritas

Subang-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis

dampak insiden, serta pemulihan pasca insiden keamanan siber pada Pemerintah Daerah Kabupaten Subang.

Subang-CSIRT melakukan penanggulangan dan pemulihan atas permintaan dari konstituennya.

4. Kebijakan-Kebijakan

4.1 Jenis-jenis Insiden dan Tingkat/Level Dukungan

Subang-CSIRT melayani penanganan insiden siber dengan jenis berikut :

a. Web Defacement;
b. Distributed Denial Of Service (DDOS);
c. Malware;
d. Ransomware.

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

4.2 Kerja sama, Interaksi dan Pengungkapan Informasi/ data

Subang-CSIRT akan melakukan Kerjasama dan berbagi informasi dengan JabarProv-CSIRT, BSSN selaku Gov-CSIRT dan CSIRT atau organisasi lainnya dalam lingkup keamanan siber.

Seluruh informasi yang diterima oleh Subang-CSIRT akan dirahasiakan.

4.3 Komunikasi dan Autentikasi

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

5. Layanan

5.1 Layanan Utama

Layanan utama dari Subang-CSIRT yaitu :

5.1.1 Layanan Pemberian Peringatan Terkait Keamanan Siber

Layanan ini dilaksanakan oleh SUBANG-CSIRT berupa pemberian peringatan adanya ancaman dan insiden siber kepada pemilik sistem elektronik dan informasi statistic terkait layanan.

5.1.2 Layanan Penanganan Insiden Siber

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

5.2 Layanan Tambahan

Layanan tambahan dari Subang-CSIRT yaitu :

5.2.1 Penanganan Kerawanan Sistem Elektronik

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

5.2.3 Audit dan Penilaian Keamanan

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

5.2.4 Analisis Resiko

Layanan ini diberikan Subang-CSIRT berupa analisis resiko terhadap insiden keamanan siber serta pemberian rekomendasi teknis berdasarkan hasil analisis tersebut.

5.2.5 Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Dalam layanan ini Subang-CSIRT mendokumentasikan dan mempublikasikan berbagai kegiatan yang dilakukan oleh Dinas Komunikasi, Informatika Kabupaten Subang dalam rangka pembangunan kesadaran dan kepedulian terhadap keamanan siber

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt[at]subang[dot]go[dot]id dengan melampirkan sekurang-kurangnya :

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

7. Disclaimer

Terkait penanganan jenis malware tergantung dari ketersediaan tools yang dimiliki.