RFC 2350 UNM-CSIRT

1. Informasi Mengenai Dokumen

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

Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 19 September 2022.

Daftar Distribusi untuk Pemberitahuan

UNM-CSIRT.

Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://csirt.nusamandiri.ac.id/download/rfc2350.pdf (versi Bahasa Indonesia)

Keaslian Dokumen

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

Identifikasi Dokumen

Dokumen memiliki atribut, yaitu:

Judul	: RFC 2350 UNM-CSIRT;
Versi	: 1.0;
Tanggal Publikasi	: 19 September 2022;
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Universitas Nusa Mandiri-Computer Security Incident Response Team
Disingkat : UNM-CSIRT.

2.2. Alamat

Jl. Raya Jatiwaringin No.2, RW.13, Cipinang Melayu, Kec. Makasar, Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta 13620

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

(021) 28534471

2.5. Nomor Fax

-

2.6. Telekomunikasi Lain

(+62) 87878799851

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

csirt@nusamandiri.ac.id

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

Bits : 4,096-bit RSA
ID : csirt <csirt@nusamandiri.ac.id>
Key Fingerprint : AEFE65ACDC9047CA1AD626A32ED0E1B8C6D805FC

-----BEGIN PGP PUBLIC KEY BLOCK-----
mQINBGMjEJ0BEADQo2ksyW9VoMyS6sgpGGKRGWjT9xfH6nFwHoVk9nIUUWQQXVu1
2sgACkalv7npunmBUMR8BX9H0fo+NJO6pwVJN2IZ88nJxRz+c+dKgsvVQUl4E4KP
iGA5+9k/L2RO5k0iWOoDS04QLZRrdi52NdlXjDrthEIsiH4OyqYZCbuseyY3jmJ5
odg6+/kPbsmR0Csnk2cXDlrV4CyRUm8WpL4UnC0hfGvRsaYY6yfN4VhAArNZ3iWs
r+yvIN7YX4dHHFjHu50p0bGXaUHLnbsRcct/Xnzu1Uh6rPmx5E/geYaJzlrZzMOD
H9mgB0A4RAerJoMVpdyqfNzR1LlIzcadHHn9xsqYe9+6fyPDLAtX4+6Glv7USbXk
tzQh9DP/9DWOBefd40u81cJzjT8l8vhRIoMr+rQiJKQlozrVB8c+wlibVMwk9WHU
SJB6Pp0hR1YK0KM/4H97Q8K/6yoZ4cJK3kvc4QoDchGtU5mZdMhTZKdMlyPJg9Hc
d6NHk2RwONI2KS9HGAXpMKFDnaFsOcF2u5dn67AlFC/J8TG2I4rv4v49TQpKTcIf
Aj/R+IZNBWy+63A/JJnO22liwOlwLyB3KF5yzqN9h1NTNzpq6azDAGYxNqpamLs6
GqlxCjYuPxI40rp49e5YuWGll+nMP2es0w2ucbRPn7dK1dMO6FnnmEqizwARAQAB
tB9jc2lydCA8Y3NpcnRAbnVzYW1hbmRpcmkuYWMuaWQ+iQJRBBMBCAA7FiEErv5l
rNyQR8oa1iajLtDhuMbYBfwFAmMjEJ0CGwMFCwkIBwICIgIGFQoJCAsCBBYCAwEC
HgcCF4AACgkQLtDhuMbYBfweTw//XHbcnCp5YXig8aW7xa9eDlKOoWYPN5UrdKh9
aI4g9k0zD+oWdI6rt0zjAwcXexCOI7vab8x2mCjr0XJ/nZZv7t2gZ6vf7rjBVKlG
uTNElQuv/MTdb6apQwvGL6M5vvqVX/TqbKbZLsfMdRPMKzs7YRizvksLpq96PR5j
Qwwub8Yb6ndI1LkuY+SLwfAqd5sTZ9Us9WXClXNhsnBJ5YjBBqP/zJEclVLx4qqc
3uUVw3DUFcWq+9knJSe+AKm755MnpOfev3C8cRaTlRlHlj+BUtucBnf8jqm9hdXQ
YjgPJ6DAI9DAv8vJnKDyiIRfsWrNnEOtZacrPCToQFBpgcxRTGXPFBaT7p8NdrAO
kC+8/ZQdzZG1deddLjctuMK8ViDVq2AuwLaUwkbrjFuNsMMkoCD3QEH0cTwGSrIo
WtBIGCpVl6Bsc3ylnqpWGQiy7571AzWUbGSYXUJuoaO6a5Z83C6SkaYiUNipTomF
/LmQGGOmCgGpZ8iezXUgTq1NEPzLXh1+xNWlEr50aOMcOTPoOAzGwwP480Pi270z
SUiwBdBWold4h+ueH0Ce/XVkJB9hSjlWgJtLEgn+6+2pjA83sGhhhgLl0f8lTVgU
YLPiJTLtRFvhasC853FF2fnLFf7/p+s+lpN/aPNxvo4QDbkayU4c3F3bInVoJ6bd
t4FlQ+a5Ag0EYyMQnQEQALC4QnrjKWFsAdBGW9qLRXsjQTKrdnkR6XQKe+Gli0Dc
bH5GAcTJO0434lPrryAb8gTQQkqc2aqxs02r7uA2mVgR3KbPrhEOgDsn5U30rfRJ
7kzMK3n7DQljh/BldeqclbBZqSxUReM7x11iLJI7eBR1B6b3Hj5EhPHNG0PF+yfT
WFTVTV66Mo1g6qUJo1ups7amsX0mZ3fp6cxxCe7PCzBw7wjY7byWn7Kzk0Usaz5P
sNMFuVifw7ZOF5ke9F7fULr9d+j8oSdSjbXOSz3RE4kZn/BgmPAV10QSr0Yfb8fx
2Y2KHnRPRfTcJUJkI4pJdTXjaElhgtH6hXwUqwG3w4unXo2XV4w7h+1xucKz+DhA
DG5DPRhp48R/cacVV9tOWkwQJ/1va63hhHYKv0ouoQqnJQ+8Im0NdXI7BVPFAKsB
/0KqMJg4LZErRzBZkZJG3qdj/67JgPr7oE21SlDlmr0hlEMM7TF/KLozOtJjXg5z
YncLxL87vNRdgoS/owLyQffbUxJZMhrqt2k3E4lM904iltaCeiGEhDoTkUsRaliV

CNpXFPFZzavN03A9vO5ZHKnUbqTVDis3B63jLZ5KT/Pcp8aotcPL5LGTlhcPP5+L
DfdMNZoRJk7TMBHHxnNfk+ET9kkH7QNLp0lZ8LTlhsl8A8zlnlohk0Q7jqKVK0JJ
ABEBAAGJAjYEGAEIACAWIQSu/mWs3JBHyhrWJqMu0OG4xtgF/AUCYyMQnQIbDAAK
CRAu0OG4xtgF/J9+D/4zD9iEo/GqzvsbG51uFMtXGBjoORNG9vVopkut5LCTqI63
8YPovefaDWigCM0LxM1n4laLxwzECzUCGsLf0YtvhA/C+mgGTdJt+ZTQKVo8lHYz
kVgNXChbBNvHucwA42OUa+74r9To7L1J3zlISPa2qx4T2Qkxc1FN0OCwI0i8k4/w
xU5hlwqb3zU/2qzBoTzEMVtyk93t+c5sxm+2t/mai6IdKG87SAWkAOUZ7FJSiCNd
yxgX+x38bAaSgPFsz5V70jiBF8+b6lHQ56kuoQueUkCOLD4h2sYQKBoRSnb8EjHu
CNcXhz1083yw7lVfNhlIH7rRfx0dvxFgVVNwBsLCpmHxy6YB5CJWrmKR7piyxzg3
WZqzzFTFfk08m3aHBKPoSIhwJzKrMyu0ayrnxJvgtzM4bzo5RRl/z1HwRUdAvJ7W
cyFN1pN31M34956fWaDjORsRUeU9Bh/CqybzJOQbc4KoNKZzUqC5hHT/toe4W80g
AUE1ZgDeXPoRfSUtJKFl0pYBsqX6Bk3lZH9W9V0z8liDSLi88uOukbud/LOYCfwB
Le4o6EnecYWvlCQi6Y0JBALrgA28L2g/+00Wx8Rgvay2UIW6xRrydOnKQEUNCV5E
+fDnbY3MGsYqghk/p2uPvdD/d2SVbtF23We1InCtXZ1TpqUCHUiY+9PE12VSow==
=zXnW -----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada:
https://csirt.nusamandiri.ac.id/download/unm.asc

2.9. Anggota Tim

Ketua UNM-CSIRT adalah Sumarna, M.Kom. Yang termasuk anggota tim adalah Ganda Wijaya, M.Kom, Herman Kuswanto, M.Kom, Faruq Aziz, M.Kom

2.10. Informasi/Data lain

Tidak ada

2.11. Catatan-catatan pada Kontak UNM-CSIRT

Metode yang disarankan untuk menghubungi UNM-CSIRT adalah melalui *e-mail* pada alamat csirt@nusamandiri.ac.id atau melalui nomor telepon (+62) 87878799851 ke UNM-CSIRT yang siaga selama 24/7.

3. Mengenai Gov-CSIRT

3.1. Visi

Visi UNM-CSIRT adalah Terwujudnya keamanan siber pada pengelolaan Teknologi Informasi dan Komunikasi di lingkungan Universitas Nusa Mandiri.

3.2. Misi

Misi dari UNM-CSIRT, yaitu :

1. Membangun, mengoordinasikan, mengolaborasikan dan mengoperasionalkan pencegahan, penanggulangan dan pemulihan terhadap insiden keamanan siber di lingkungan Universitas Nusa Mandiri;
2. Membangun kerjasama dalam rangka pengamanan siber terhadap layanan TI di lingkungan Universitas Nusa Mandiri.
3. Meningkatkan kapasitas sumber daya manusia terhadap ancaman keamanan siber pada aspek pencegahan, penanggulangan dan pemulihan insiden keamanan siber di lingkungan Universitas Nusa Mandiri.

3.3. Konstituen

Konstituen UNM-CSIRT meliputi seluruh satuan unit kerja di lingkungan Universitas Nusa Mandiri.

3.4. Sponsorship dan/atau Afiliasi

UNM-CSIRT merupakan bagian dari Universitas Nusa Mandiri sehingga semua pembiayaan dari Universitas Nusa Mandiri.

3.5. Otoritas

1. UNM-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber dilingkungan Universitas Nusa Mandiri.
2. UNM-CSIRT dapat berkoordinasi serta bekerjasama dengan pihak lain yang mempunyai kompetensi untuk insiden yang tidak dapat ditangani.

4. Kebijakan – Kebijakan

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

a. Web Defacement;
b. DDoS;
c. Malware;
d. Phising;
e. Pembajakan akun
f. Akses Ilegal
g. Spam

Dukungan yang diberikan oleh UNM-CSIRT kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden. Layanan penanganan insiden berdasarkan pada laporan konstituen.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

UNM-CSIRT akan melakukan kerjasama dan berbagi informasi dengan CSIRT atau Organisasi yang berkepentingan dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh UNM-CSIRT akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, UNM-CSIRT dapat menggunakan email tanpa enkripsi data dan telepon namun untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi pgp pada email.

5. Layanan

5.1. Layanan Utama

Layanan utama dari UNM-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini dilaksanakan oleh UNM-CSIRT berupa pemberian peringatan adanya insiden siber pada sistem elektronik dan informasi yang dikelola oleh masing-masing satuan kerja dilingkungan Universitas Nusa Mandiri.

5.1.2. Penanganan Insiden Siber

Layanan ini diberikan oleh UNM-CSIRT berupa koordinasi, analisis, rekomendasi teknis, dan bantuan kunjungan ke lokasi dalam rangka penanggulangan dan pemulihan insiden siber.

5.2. Layanan Tambahan

Layanan tambahan dari UNM-CSIRT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini diberikan oleh UNM-CSIRT berupa koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan, UNM-CSIRT memberikan informasi statistik terkait layanan ini. Namun, layanan ini hanya berlaku apabila syarat-syarat berikut terpenuhi:

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

5.2.2. Penanganan Artefak Digital

Layanan ini diberikan UNM-CSIRT berupa penanganan artefak dalam rangka pemulihan sistem elektronik terdampak ataupun dukungan investigasi.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Pemberitahuan hasil pengamatan terkait dengan ancaman baru Layanan ini diberikan oleh UNM-CSIRT berupa hasil dari log perangkat aktif yang digunakan oleh UNM.

5.2.4. Pendeteksian Serangan

Melakukan pendeteksian terhadap berbagai serangan yang terjadi dan di pantau melalui sistem deteksi dan monitoring keamanan.

5.2.5. Analisis Risiko Keamanan Siber

Layanan ini berupa identifikasi kerentanan dan penilaian risiko kerentanan yang di temukan. Selanjutnya di berikan rekomendasi yang dapat dilakukan untuk mengurangi risiko tersebut.

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Pemberian konsultasi terkait kesiapan penanggulangan dan pemulihan insiden keamanan siber.

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Sosialisasi dan pembinaan kepada seluruh unit di lingkungan UNM yang bertujuan untuk meningkatkan kesadaran dan kepedulian para pegawai tentang keamanan siber.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt@nusamandiri.ac.id dengan melampirkan sekurang-kurangnya:

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

7. *Disclaimer*

a. Sampai saat ini UNM-CSIRT hanya merespon dan menangani insiden keamanan siber yang terjadi pada perangkat kerja yang ada di lingkungan UNM;
b. Terkait penanganan insiden jenis malware tergantung pada ketersediaan tools yang dimiliki.