RFC 2350 UNY-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 10 Maret 2023.

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://csirt.uny.ac.id/rfc2350.pdf (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

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

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 UNY-CSIRT;
Versi	: 1.0;
Tanggal Publikasi	: 10 Maret 2023;
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

UNIVERSITAS NEGERI YOGYAKARTA
-COMPUTER SECURITY INSIDENCE RESPONSE TEAM
Disingkat : UNY-CSIRT.

2.2. Alamat

Pusat Teknologi Informasi Dan Komunikasi
Universitas Negeri Yogyakarta
Jl. Colombo No.1 Yogyakarta 55281

2.3. Zona Waktu

D.I Yogyakarta (GMT+07:00)

2.4. Nomor Telepon

+62274-545097

2.5. Nomor Fax

-

2.6. Telekomunikasi Lain

+62-274-586168 ext 228

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

cisrt[at]uny[dot]ac[dot]id

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

Bits : 4096
ID : 0xAC42C89677FFA31E
Key Fingerprint : FB77B17129E75531060F4642AC42C89677FFA31E

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

mQINBGQ5AEoBEACtm0JGjTCHmozE+/pJoHfBKcD8EPjWvz9Bu3BpVHiYDRjyr0b4
GGiWuOsX6iba6bk1Hqyd1ms9Wnupzc3qWMmrGbE+a4TBWWMD39w+SouKbAatBYRm
I5RFXPzZuMJP9dmA2kdXH3iLeY+ADc5UxVPl9YF5kmV7oCMiTPWoD+6CHR3wnyNj
UIwvDsPEFQv/IJcS0YvmQXHAdj5fM14NmxFQjtTMvGYf9BjtmzGz6Qn/zFZRIVgr
A9irUwIqB2hRVYYW6qIlogJvGQnZklPquFHQ8XifVDnlZACcaBN4po4dkB0Zio2P
6mF9ds3xLxkoWqMK5w+CQhpzfON0ufIDoT/ekb0dG39QWof+9KjDqrE/vhltX3z0
PIMWi+C2cKucHm5LDHCq7wMMleM6QJ9z+W8FdTbEkLQNqS39e1Lv1S+u9wTw17th
aaLyVIaP8TmH6RxS0vHSgqmPu80PvNyHifSVJh+0cjRjjD69blKbmgnV5RivD/Hr
UdDkK0RhwnxKnQNv8cJdqdqUldLqc5LZuQqo5RA8LLz37daIKdnrb9QjXTX4K46z
l2uTAMzBemzcWg1ruEW0XPmzX5nKSYi3XndVY1QpDYmg57vWJ+WD9rZawWCVhbHI
zNi7h0n6woynBnzpwMMo+prLdUDtr2V3Qyjq00h3pYbUepOFcCNFYJbtDQARAQAB
tCdDU0lSVCBVTlkgKENTSVJUIFVOWSkgPGNzaXJ0QHVueS5hYy5pZD6JAlcEEwEI
AEEWIQT7d7FxKedVMQYPRkKsQsiWd/+jHgUCZDkASgIbAwUJBaOagAULCQgHAgIi
AgYVCgkICwIEFgIDAQIeBwIXgAAKCRCsQsiWd/+jHrkqD/0XVvnuNyaZmWsY5+YQ
7kxVGGz/GfAoSOQAnnlc6ERb4XTLdCxqL+LRgN8VN29RA9so5CSh0/hP5oCzt40n
6hDREa6odBXKRocJSu3zC6hQaSAvIvmmvOuaIbO0d4IDRO5KsRnNtR4zTaD2KDRy
91zj5mVvFNiBJeDcIhLrPXxzksKpkPKqMRwCOZGhGYmOXWGBpXmi43aan7aS9gS4
VVEaL2EUJk85tQPTMGB6cPdkBNz0rJnu9k/uPRvXIEkwWdOs5RgeV5ftSAun/RhR
RDxTFlxpDgLWFaq6IXI/PdJY0aikWUYOpw07nJzV90fFkVb3ZOiO1RWJal3joIIO
4FjnreIU+q03elRTj0MfAWMbwHaac3gZ8V2MrY+i3Lv0VzRmi7l9x8XAcNuRzCk3
0yaHNoUp6V1fuvxTtKEqqiBfYJ19Q/rVy57RbwIDScxEk84iSA2DLWmo0nP7TCku
fb1oBD3SR+N95KNrJPiwj3CMI2GKd7U/L7At5b0wNI5n6vG6lY478gNPPG3pelg9
n4QLT/dsoP16oN6UKxd2ZJFVKXokA7Frd1dic05xxVIeYWngaS3jA1y79jt/e0Xr
zWV3voT3RWjfL2TN0a63UE3pAij1UK/98nKd5qsPTuYaases9ailaYsBFNBH8O+m
kGKpzeb5f0SSEiuZ8IceCEb7kbkCDQRkOQBKARAAoECA43w5glp9juhefKThw7Wr
dd2syV2yUApyL/PPaeoK8dzUV1Fj46gWy1euYfQMZa4EiuSXVdLYR1YfYiE25sBU
SsGhxcji84mmUV7pHYvI7+CMcfxKiZ8r/0PphkYPiAE61KMZTco4QA7tN3lEZe68
MkWlh5Debgvz1Intm5PUBMvDf8WNRBnKhZ5Kuj8PitWI8NQKdbWaz1CsxtHt3UE7
LI04CqLS3ioKQhaJU5WnjxGWqUy+v5jBsM3uoQAB/IJ+OtGw2pEtwKxyI6hZvVx2
YlZUXONTUch5zyHrCuEj3ARHW0njyRaHjMNnfpRd+vFELk8ufzgEiIw4Y0gcblSG
lywBvFwXaF82Z8XufcR4qQPoBc3CkgVU7948MvE7kV7Cp5T2U6QDK7r5bfe3XRJg
SUqJHrw84FWK4aG+XfWNiMA4J7K8Z571XNNKrE2B5HpLgYOZ/l5rOHgfUn5ixwtM
DioCYQUiYJhsjATeUAocQZD1r/NVaNpYnbfjLMrE7d/Ojg/gCswBnvAVLMHGmg51
BfKEd3kG9RelS0xYp09S8f6rzSN4d5E+p5P3983tvQREnkMyITkoEll2M7lCYkBb
k4AFzKHZG+ULR811DmN6F5PbAe2lrvcVMlqyp35/8CD6f/HGXhMz+lnW4TJOX7mJ
jCRGMa9LL7jy9U8Sri0AEQEAAYkCPAQYAQgAJhYhBPt3sXEp51UxBg9GQqxCyJZ3
/6MeBQJkOQBKAhsMBQkFo5qAAAoJEKxCyJZ3/6MeCLgP/irDesOj+qY9BE3KPrjI
u426ZixaOJW/ZiGuHHc36PQVGLLKkXA7XGO8Z9LKOZzvyKSJSjxwUQVMYaXYbKFl
/LJFVE3vfW7jOT6PmwPoY3A6HQBawX+iQ4LczSGmQnpWgQagAZUOAHxWV+lFDBbJ
hGzQCYGg4QjcV7/xUYWC6M+prPVu6n1W+l8nJkycXxCd9SoO7XCI5Yy4zi/6F4en
3/Ry7aUkwR4+vX8KuHBpXgURIAQh17yy4+PGi4DxLcTbQm8AYvTqKCiMoohZCtDi
Ey3Z2635y/LLwdAXHVIj7CHiKxJQJlVA7H04kwHNTjOZ+MLwDlgowRRSqUE57hMb
+lQQjBvidMlrHhXBzX4WEpoGtr1ypRucDrbwPqdeaKhVTzLgugwq4K/H5b6C9wGN
64mwudi/Yx28HGCYHH4kSrJli+zGNuuqi3BaC3ISNnICMovijO6CIDrP6j6Q4YJq
7oeYc3wh1J97h1pLT9ye2ZR9P1NzPndO9VnXBBnJBlnxFQN+9mMpJYRV3/EUTHGZ
fjVfoQF68b+2eOMTjcAyoNVOaEsaw7vM8LGi/9cT18B3DT000hRfYKVPL4z65dyd
BXfVyiAylAjIldNjMqUw7AsYKf+Z1PHcJ5dAQPGdNaYeGK9eXGVQSEwQC51mu7Bb
VHDqZDvZ6q8HuRYd+MoEQVKr
=/37F
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://csirt.uny.ac.id /publickey.asc

2.9. Anggota Tim

Ketua UNY-CSIRT adalah Kasubdit Sistem Informasi dan Keamanan Siber UNY dengan anggota tim adalah seluruh Tim Divisi Sistem Informasi dan Jaringan di Pusat TIK satuan kerja Universitas Negeri Yogyakarta.

2.10. Informasi/Data lain

-

2.11. Catatan-catatan pada Kontak UNY-CSIRT

Metode yang disarankan untuk menghubungi UNY-CSIRT adalah melalui *e-mail* pada alamat csirtat]uny[dot]ac[dot]id atau melalaui pengaduan di laman https://cisrt.uny.ac.id/pengaduan

3. Mengenai UNY-CSIRT

3.1. Visi

Visi UNY-CSIRT adalah mewujudkan kampus dengan ketahanan siber yang handal dan profesional.

3.2. Misi

Misi dari UNY-CSIRT, yaitu :

a. Menjaga keamanan jaringan komputer dan sistem informasi di UNY dengan mencegah serangan dan merespons dengan cepat ketika terjadi insiden keamanan.
b. Menyediakan dukungan teknis dan bantuan yang cepat dan efektif kepada pengguna di UNY ketika menghadapi masalah keamanan.
c. Mengembangkan kebijakan dan prosedur keamanan informasi yang memadai untuk melindungi data dan informasi penting di Universitas.
d. Meningkatkan kesadaran tentang keamanan informasi di kalangan staf dan mahasiswa di UNY melalui pelatihan dan kampanye kesadaran.
e. Memonitor dan menganalisis jaringan komputer di UNY secara terus menerus untuk mengidentifikasi potensi ancaman dan mengambil langkah-langkah pencegahan.
f. Berkoordinasi dengan CSIRT di organisasi lain di dalam dan luar UNY untuk berbagi informasi dan sumber daya dalam menghadapi ancaman keamanan yang lebih kompleks dan canggih.

3.3. Konstituen

Konstituen UNY-CSIRT adalah seluruh civitas akademika Universitas Negeri Yogyakarta

3.4. Sponsorship dan/atau Afiliasi

Pendanaan UNY-CSIRT bersumber dari Anggaran Universitas Negeri Yogyakarta

3.5. Otoritas

Memiliki kewenangan untuk melakukan penanggulangan insiden mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber pada lingkungan Universitas Negeri Yogyakarta.

4. Kebijakan – Kebijakan

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

UNY-CSIRT melayani penanganan insiden siber dengan jenis berikut :

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

serta dukungan terhadap konstituen tergantung dari kasus yang terjadi berkaitan dengan keamanan ruang siber.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

UNY-CSIRT kerjasama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber dan informasi/data akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

komunikasi biasa UNY-CSIRT dapat menggunakan alamat e-mail tanpa enkripsi data (e-mail konvensional) dan telepon

5. Layanan

5.1. Layanan Utama

Layanan utama dari UNY-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

peringatan diberikan kepada seluruh stakeholder di lingkungan Universitas Negeri Yogyakarta dengan memperhatikan tanggung jawab masing masing stakeholder yang ada di lingkungan Universitas Negeri Yogyakarta.

5.1.2. Penanganan Insiden Siber

1) Identifikasi insiden: Mengidentifikasi dan memverifikasi adanya insiden keamanan informasi, dan menentukan tingkat keparahan insiden.
2) Respons terhadap insiden: Merespon insiden dengan cepat dan efektif, dengan mengambil tindakan yang sesuai dengan tingkat keparahan insiden.
3) Investigasi insiden: Melakukan investigasi terhadap insiden dengan tujuan untuk mengetahui penyebab insiden, kerusakan atau akses yang terjadi, dan dampaknya pada sistem dan informasi.
4) Pemberitahuan: Memberikan pemberitahuan tentang insiden keamanan informasi kepada pihak-pihak yang terkait, termasuk pengguna dan manajemen.
5) Pemulihan: Melakukan pemulihan sistem dan informasi yang terdampak oleh insiden keamanan informasi, dengan memastikan bahwa sistem dan informasi kembali dalam kondisi yang aman dan terjamin.
6) Evaluasi dan perbaikan: Melakukan evaluasi terhadap tindakan yang telah diambil untuk menangani insiden, dan melakukan perbaikan pada kebijakan dan prosedur keamanan informasi yang ada agar tidak terjadi insiden serupa di masa yang akan datang.

5.2. Layanan Tambahan

Layanan tambahan dari UNY-CSIRT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan penanganan kerawanan sistem elektronik ini dilakukan dengan monitoring, analisis dan rekomendasi yang akan disampaikan kepada setiap pemangku kepentingan baik internal maupun eksternal yang terkait dengan UNY

5.2.2. Penanganan Artefak Digital

Layanan ini berupa penanganan artefak dalam rangka pemulihan sistem elektronik terdampak ataupun dukungan investigasi dengan memberikan informasi statistik terkait layanan di lingkungan UNY.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan pemberitahuan hasil pengamatan potensi ancaman yang dimiliki UNY-CSIRT ditujukan kepada seluruh sivitas akademika UNY, baik mahasiswa, dosen,tenaga kependidikan maupun pihak eksternal yang ada kaitanya dengan UNY sebagai pengguna layanan teknologi informasi atau pengguna sumberdaya yang berada di lingkungan UNY

5.2.4. Pendeteksian Serangan

Layanan pendeteksian serangan ini menggunakan menggunakan firewall yang telah dimiliki oleh UNY

5.2.5. Analisis Risiko Keamanan Siber

Layanan analisis risiko keamanan siber dilakukan oleh UNY-CSIRT menggunakan berbagai sumber data yang dimiliki oleh Badan Sistem Informasi UNY.

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Layanan konsultasi terkait kesiapan penanganan insiden siber di lingkungan UNY dilakukan berdasar permintaan dari stakeholder dan pemangku Kepentingan di lingkungan UNY.

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Layanan pembangunan kesadaran dan kepedulian terhadap keamanan siber dilakukan oleh UNY-CSIRT adalah dengan memberikan edukasi terhadap user dan stakeholder terkait ancaman-ancaman dan dampak dari insiden keamanan siber bagi individu dan institusi.

6. Pelaporan Insiden

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

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

7. *Disclaimer*

Penanganan insiden tergantung dari ketersediaan tools yang dimiliki oleh Universitas Negeri Yogyakarta.