RFC 2350 *AMIKOM-CSIRT*

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 10-08-2023.

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.amikom.ac.id/rfc2350.pdf (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

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

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 AMIKOM-CSIRT;
Versi : 1.0;
Tanggal Publikasi : 10 Agustus 2023;
Kedaluwarsa : valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

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

2.2. Alamat

Jl. Padjajaran, Ring Road Utara, Kel. Condongcatur, Kec. Depok, Kab. Sleman, Prop. Daerah Istimewa Yogyakarta 55283

2.3. Zona Waktu

D.I Yogyakarta (GMT+07:00)

2.4. Nomor Telepon

(0274) 884201 – 207

2.5. Nomor Fax

(0274) 884208

2.6. Telekomunikasi Lain

-

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

csirt@amikom.ac.id

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

Komunikasi melalui email dapat menggunakan PGP. Adapun public key CSIRT AMIKOM adalah sebagai berikut :

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

mQINBGTR56IBEADFJFhisPGWdxAgA+GMzX31wPEStEMdFv1LM2b4Vo8YVkXU5/NC
D+W37Jgi38LgsN5uGRt4NbaBCzQT3kF5H9SuvZ3R0qIWCwDEwUW2SKU0nQzwsU/i
hQRXZWLLo3X6mT87FitaIK6y4dLnYSCXkrjWC6NVQGzOnJQWOCFikA14l0Moj0Qv
SmeAgM7yaN+ZdC9V4xNrUF+jy4c+RUvr1F0EyHyDtWewU5WMVURSPke2WSTpTu2m
ho07+mGNaRVvOvO//oCWcgDfQUK4+8wEzjC+niNjYiL/IdI2vhdGpH6hzvLNBYs5
tbn89PoffCHYvOnJAbSgdU/1ERrkG6H1N+1Pby0VokmVnsbUaaZqBUQsldpdQw42
ru5tIOdK4GGUri17DaTssbP7F9OxXgt4TzUaT8ZZF79G2TrEXQUuKepM+DymelfT
SCj8G+c5M0vkT0tEBJvpjYNvu1jRqbKJKB6TEv/TwUhB1A8TJ5nE6STFmU3P+Re
N
GxkQWj5gBSk3XPaGfruJ/YGgoE/nd4gLG27vnAU6QXn21zJFcgZL8auaoUfssaI8
dRgEiSNtfiZ5fKZ8yPtloykSZZFetgg4CtMXtON7GyYi+cuo9u0bvr3jVxXBlRdu
lqJEvGIVD0uHfhtIQJZY37G6Su5rDpj3cb1Ils2f6AEsL9ymX4q/FRRzMQARAQAB
tDNDU0lSVCBBbWlrb20gKERhdGEgUHJvdGVjdGlvbikgPGNzaXJ0QGFtaWtvbS5h
Yy5pZD6JAlcEEwEIAEEWIQR5xDTC7A+H89tOqo8JMEQZ99u9UAUCZNHnogIbAwUJ
A8JnAAULCQgHAgIiAgYVCgkICwIEFgIDAQIeBwIXgAAKCRAJMEQZ99u9UNU8D/0d
W517WUVEmj6JmadpkZ0rQWN+nd3DvZwCMdbSwgqbMqQPMV+hZrNKrKw3iIad4dT1
TUlJpk3o0G6rluO6jfdpCmzwwWK4puMkYof80wbNkyxJtGfJWg/Mb/8banycIGTj
0P/p8vJA2wJMRaFrw09Abxep1ri98IBPypgtq7Ncca0u+R3UOtkuyKLOT3YQvYbX
R9uY8PnN6TuayWQI13M6KphjHSBmxC8rK3miUAPaYRmfT6C6PVqv005AUuTh8TdI
IeBluZkBnWgoka4WgrsTm5mV2BpW+9Evg/cA3eDPvO1nCYwpltBSueIhNJIUKTA0
pp8RpzdkRMbbFSFCdqVlnMbdRxQs1qjrhWbKdldr5b7ayj0TjnPqe0wm4lGvr2yO
qC6eQpWN4+wwyyC8a6V9XYId7Hz/chb0j3fpjnPPWUwqiCrJiOSF23e4eZ+RpMnO

ZK6KiBJV2MHe7flKyzwzX7yxys7BnA+wMmSwURhHUtDh3hyWJmMMgh8ZMzN0iv3Q
J2DEmOXgoD1DksxxTKUzTfGoVsmlTrA0b6sknJuoRAiPOOJkIxBNJPuUTwA2oMQi
0TOcSHMuWu7Xj6lmOgNgZTupWtzFHCxAZIoTREoiU1Tmknxv8QR4kqQilxNHE6wY
3wdNHkTZflY/0rKD/LniE4adhI8rqH7QSkH45r7xkLkCDQRk0eeiARAA0AqrW43U
DR5xwZpjpj393l7ayA0yBaNvMA0TIy0WUh1QOwN24Dw8ik2E7gE0St5xBFGFY3bT
2WMuj+TW0E1ZV+jqnenu3aKdfYz/5f/h0jjos94niUeMfZ5JVqZ/6ZkkV48PBLQk
GCtlVQstzhg0kRd+OBH3NFa6Jztfos+75i1zTyLuO+MdpsOhP/29rPV1lQFJ4NFk
qEGCMi4jJ7mPUshtooq4Xp6zhP0bUGJMtOALY2EZFGi8av2VKf9q5F5bup1uhX4+
MoM7ZxoU8vAOrRq5lKIc6lnaMZh3GQFrthEa0Kne2AomuvTUIGa3vrOBFcUXHQ9U
8ucM7AtxFa0ZDDPNT0RzdMUSQWeK4K5ToCTTXHLUxEm7Gjaw2Hogc0mui2ToS1Es
Bd1uyWxr4yrp2uy4Cy074qMtvS0m3pab/OfMcGtEx9VY7MBXojihPJR0DFOFdJeV
ErrJSO2LMNEXRNCoA5OuAEui702Tc/XobpwEZ54VVnkH9vQ6Nl3s7ZYEwlUZelCa
n4VFETHDOp5K2/B1k+q4Iu6c50W4bI1QXkMWDhMTpITzzFMMIPhwYKLyYjoWo8Gd
4kIZbT31E/GR6qHMn9QxAvrSXZDy0lN/ubIk2GMXuoR2T81TvCjikdvdo6bJfwXE
hqtdZed8drv+nhAmg9hjNPO9OGQf1IiByikAEQEAAYkCPAQYAQgAJhYhBHnENMLs
D4fz206qjwkwRBn3271QBQJk0eeiAhsMBQkDwmcAAAoJEAkwRBn3271QFUAP/2dr
q5nxQY0jSiQCaLWc2ZOrnrOB5Snm4ENP1fxeHuxiih+695QsYNSsIpHIGEBDtjWh
TuXINGoN3ReBcJHCumYVYIYr1ZKsqzsqMmnm1m1h+ZWixhmqHH85bijNrIo9osqn
EjISGLxfIHHSzdG4gNGGmvwhGYq/bTHooksQZblSsowDYgEYx/9J6IBNhhoYIjcP
ADoW6n9uqQxO3435mDOHg7fk/988mWctZHldSi6T3CG/28QhnRBczWW3AaNtt0Yt
KLMKWpCP4Vc0lP+EP39GWPH2P79egQ11cbofrZPaw/coFYw3JeI7OeZunn+FQ4Ww
4EctOefdncLgk8Hl8RsNPQvT/m77pV71Js3E4lcQDFdQD866VBOEFzRp43qWb37n
7m8l22p2A2dcs+WMEFFEU2py3ey0F0gbHsWZYUfSpGBbmLiAgZjUoFFN811EWA7A
gvVm8hxKqZNCKfCs5KG5k2YxHKEpRzGX2e0ztDOZCeMZl8NIcMO3hIOpZENyrgg1
Zc+7m05yGfQJWwGFnngDGnxcM+65HUcGt7dpCYTCgHYeRcspe1ATyzjXobDVxpsQ
Ngw6b9u9rL/0aIibpbc9GdyIZLoGMnawpr6+13x/I2VaN35NusNyhF+vQW3gVVS3
RTNAGZ/TSvh/yf0F/mjR/gDdSBJlKvQWT1XIJwxO
=kPFP
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://csirt.amikom.ac.id/ca-pub-amikom.key

2.9. Anggota Tim

Ketua AMIKOM-CSIRT adalah divisi Infrastruktur dan Jaringan Innovation Center AMIKOM dengan anggota tim adalah seluruh tim divisi Infrastruktur dan Jaringan Innovation Center.

2.10. Informasi/Data lain

-.Tidak ada

2.11. Catatan-catatan pada Kontak AMIKOM-CSIRT

Metode yang disarankan untuk menghubungi AMIKOM-CSIRT adalah melalui *e-mail* pada alamat **csirt@amikom.ac.id** atau melalui telepon (0274) 884201.

3. Mengenai AMIKOM-CSIRT

3.1. Visi

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

3.2. Misi

Misi dari AMIKOM-CSIRT, yaitu :

a. Menjaga keamanan jaringan komputer dan sistem informasi di AMIKOM dengan mencegah serangan dan merespons dengan cepat ketika terjadi insiden keamanan.
b. Menyediakan dukungan teknis dan bantuan yang cepat dan efektif kepada pengguna di AMIKOM 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 AMIKOM melalui pelatihan dan kampanye kesadaran.
e. Memonitor dan menganalisis jaringan komputer di AMIKOM secara terus menerus untuk mengidentifikasi potensi ancaman dan mengambil langkah-langkah pencegahan.
f. Berkoordinasi dengan CSIRT di organisasi lain di dalam dan luar AMIKOM untuk berbagi informasi dan sumber daya dalam menghadapi ancaman keamanan yang lebih kompleks dan canggih.

3.3. Konstituen

Konstituen AMIKOM-CSIRT adalah seluruh civitas akademika Universitas Negeri Yogyakarta

3.4. Sponsorship dan/atau Afiliasi

Pendanaan AMIKOM-CSIRT bersumber dari Anggaran Universitas Amikom Yogyakarta

3.5. Otoritas

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

4. Kebijakan – Kebijakan

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

AMIKOM-CSIRT melayani penanganan insiden siber dengan jenis berikut :

AMIKOMCSIRT melayani penanganan insiden siber dengan jenis berikut :

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

AMIKOM-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 AMIKOM-CSIRT dapat menggunakan alamat e-mail tanpa enkripsi data (e-mail konvensional) dan telepon

5. Layanan

5.1. Layanan Utama

Layanan utama dari AMIKOM-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 Amikom 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 AMIKOM-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 Amikom

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 AMIKOM.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

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

5.2.4. Pendeteksian Serangan

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

5.2.5. Analisis Risiko Keamanan Siber

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

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

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

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Layanan pembangunan kesadaran dan kepedulian terhadap keamanan siber dilakukan oleh AMIKOM-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]amikom[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 Amikom Yogyakarta