**RFC 2350 AP1-CSIRT**

1. **Informasi Mengenai Dokumen**

Dokumen ini berisi deskripsi AP1-CSIRT berdasarkan RFC 2350, yaitu informasi dasar mengenai AP1-CSIRT, menjelaskan tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi AP1-CSIRT.

* 1. **Tanggal Update Terakhir**

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal …… 2023.

* 1. **Daftar Distribusi untuk Pemberitahuan**

Tidak ada daftar distribusi untuk pemberitahuan mengenai pembaharuan dokumen.

* 1. **Lokasi dimana Dokumen ini bisa didapat**

Dokumen ini tersedia pada :

https://csirt[at]ap1.co.id (versi Bahasa Indonesia)

* 1. **Keaslian Dokumen**

Kedua dokumen telah ditandatangani dengan PGP *Key* milik AP1-CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

**1.5 Identifikasi Dokumen**

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 AP1-CSIRT;

Versi : 1.0;

Tanggal Publikasi : …. 2023;

Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

1. **Informasi Data/Kontak**
   1. **Nama Tim**

*Computer Security Incident Response Team* PT. Angkasa Pura I

Disingkat : AP1-CSIRT.

* 1. **Alamat**

Kantor Pusat – Jakarta

Grha Angkasa Pura I Kota Baru Bandar Kemayoran Blok B12 Kav.2

Jakarta Pusat, DKI Jakarta – Indonesia

Indonesia [10610]

* 1. **Zona Waktu**

Jakarta (GMT+07:00)

* 1. **Nomor Telepon**

(021) 6541961 ext.2161

* 1. **Nomor Fax**

-

* 1. **Telekomunikasi Lain**

Tidak ada

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

csirt[at]ap1.co.id

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

Bits : 4.096

ID : 1A1A1A12

Key Fingerprint : 1C7D 18B1 B298 7622 DAF6 8347 CE45 D819 A395 ECAB

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

xsDNBGVeyFEBDADuZZTVxlEVkbgmdMz/+bb/yRzho+qMCJA8nosFPjW8S3igGZUR

4fWzZoQHK4hLkiUGT5TTNICAY8qFC4jguTi+oxajXfEZ+mptnZ3+eMsTeCQVyohR

Rm6iOvdeOyGedsQssMYRGOjENzjZknqxVcxDRG2G/0IeneyGhjcu1YAqyPBT5QBJ

TccDPYgZUbRAjSEVDZa20T9ZnRXnX9igtcrkFNkN4NpKN6mQoBSFNz+lTbq4JjUH

iq9sYZC/+Yq+hp+kpS8osr+1FVIFk55hA+OiQmkP9z5IwKWLjYE5vJm9p+37/mo1

AmKXrVfk3Aal4Z2cD1qZJwGBxzJwWamtYZGAwaMi5AHK0BDxMcsPVjheSpglG5gP

THkVHZ9AzSMbYbA6NLe/U43Wiu2RYOZtAqQUHFsp0vUa4JhUa4a03X/5v0hOSUd8

sa5fiMfML6BJjLhFam/XXDVL9eVWx9Inoa0Hs/AUU4HdM+VmdpeNDhxbhCOT5gfm

hUQZzxaqk1ZfAXEAEQEAAc0bQVAxLUNTSVJUIDxjc2lydEBhcDEuY28uaWQ+wsEN

BBMBCAA3FiEEHH0YsbKYdiLa9oNHzkXYGaOV7KsFAmVeyFIFCQWjmoACGwMECwkI

BwUVCAkKCwUWAgMBAAAKCRDORdgZo5Xsqw+bDADODBB0dGnnZOMU9lgTe2DLigjS

tnhlFbAhw+m9pxviFOG4kwMbSflcs/3hSal1Cyj3KGNCiy7TdxG93dYli6kv90tQ

Q0DtDGzaynmDEh2hmnxsINmRr9l5qh8qlHVsGbJZqIyVxce15hCh2tywFa//uCIF

L4pl3C6lgcchU8i3UN9bIPkie0cr0zebLm9uZp0Nfc2DxcJeZBpI+nDq6pCqJS/l

5GhHWjXvImiwHG8HCaLde2DLBtxnyHWJ7LrE7Oypk9flHQxHCVLRzyYgRoSH0Mqb

dgnx+/AGanwO0+r27MLCVGi5RMCggKB/zDMFhjGlcx/2TzxNthCeqsGS1j0ydEH7

qi2/v0qdSyvTDaZ+PILt6+j1J0LcOg1MN3EnFkMxfXaNS4JzPsJdP+SAL1yQVUg5

El3qLBx0akrq5nh4A0+7eVIVblQJu2pIdmzTizJjax7vWmwUL58pp+uORAEZSawI

l75wJcz+9Y6ebacSAb9mkcuq0pbYnVoZtGOHLIXOwM0EZV7IUwEMANR0OLZvmed+

qYYCX5a6ccNm37vR/TtT1A7ZNhsvxeVEDOf0eJ9/sjDBxsmdb3yycGc7Dv1u1koq

SfQUr9c9V7CvHxfSeRcPuXCgRUIIrEYfbXKUoOahONKUtvWlwWnYTCe1Nwr+VL33

JX/YlFWCr/JjUsRVrL9jnlOx6S1Qq/ADqUFTyb+Gn6SttB6xjq4oojRbKz0u3suW

Jp3twNv5Zl/ZUND1LH56hG0pbhaggVVLTfnzJD5xGTK++HMi3ugg3JUDYXdk20Ns

e1HYVhMa6R1bhqR73vlemu09VSjr7KDlWKdo4ZrU/7OzX/h0MfAvn1VMNVQ8PQdw

HHv0HIcLQJPZafuIiVXGpYWC3+z1xMB91YZq7PiNZL7+neaIPtiGDaf3T5xhKLDM

f1SNWaYjAqEhOEwAiJpPGkQQVXxVfghhGlm4jbFSaDcm7y3/rx3A3s43N0Ybzhgz

qg6RkAaM71NLcb2ouYpEINy8RF4/pu5UvAETBdasa7ntKqhnqDiJYwARAQABwsD8

BBgBCAAmFiEEHH0YsbKYdiLa9oNHzkXYGaOV7KsFAmVeyFMFCQWjmoACGwwACgkQ

zkXYGaOV7KuPgwv+MdnrKzBA9RO6BKp/JLpOuQGgT8Unl3QzQZUNbMR29PtokgRJ

ARvVyjDtEuXaHbP92Tz6b5a/2t/fwVJgF41BlW5NReaNchGb87+hLAqXaZlKJQXv

YvE28iLeyPecBdFmE57uAXOVGQwpP93+bFaKFb60898HGCJvcmIhfpaKhXjWLoGw

gWnfd1jr9FAqTZy3Ha8VbfLdL9zvoKsk+PwTH2PiVWTx5EgWk90vgbQpUg5/snzw

uMil2eC6GjrLSmyMlyD4qNXaVW+8f3uHI/iC39OwZDa/5wVx1Qzk05YNFqdqLfBt

XboPwb9pOeQQWbB3CZn/13Uz+wN/JREvLkd5pk3RQ7VCfeJje3wPX9tTdemUEtkK

DkNXXuc0kNo9GnzlER/4PKo4LOZ/d3HdFlGxpUxu+H7jM0DnzL4zDEdyJ9TjG2Rl

u2q3JQe+dCW4HXuctUVr7WMsbqcip50MPjhhOHjpRTQ9J0nCSBdYyHhE7AKAvQzO

rOMrcTKhxxNo44ph

=8kas

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

File PGP *key* ini tersedia pada :

https://websitecsirt.go.id /publickey.asc

* 1. **Anggota Tim**

Ketua AP1-CSIRT adalah Pejabat Pimpinan Tinggi Pratama dengan bidang tugas teknologi informasi dan komunikasi. Tim AP1-CSIRT adalah Pejabat Administrator, Pejabat Pengawas, Pejabat Fungsional, serta Pelaksana Pengelola Teknologi Informasi dan Komunikasi pada PT. Angkasa Pura I dengan bidang tugas teknologi informasi dan komunikasi.

* 1. **Informasi/Data lain**

Tidak ada.

* 1. **Catatan-catatan pada Kontak AP1-CSIRT**

Metode yang disarankan untuk menghubungi AP1-CSIRT adalah melalui *e-mail* pada alamat csirt[at]ap1.go.id.

1. **Mengenai AP1-CSIRT**
   1. **Visi**

Visi AP1-CSIRT adalah mewujudkan pengelolaan keamanan informasi di lingkungan PT. Angkasa Pura I yang sesuai dengan prinsip keamanan informasi yaitu untuk menjamin ketersediaan (*availability*), keutuhan (*integrity*), dan kerahasiaan (*confidentiality*) Aset Informasi PT. Angkasa Pura I.

* 1. **Misi**

Misi dari AP1-CSIRT, yaitu :

1. Mendorong kegiatan pengamanan informasi dan pencegahan insiden keamanan informasi.
2. Membangun kesadaran keamanan informasi pada sumber daya manusia di lingkungan PT. Angkasa Pura I.
3. Menjamin keamanan informasi pada aset informasi PT. Angkasa Pura I.
4. Melaksanakan evaluasi secara berkala keandalan sistem keamanan teknologi informasi di lingkungan PT. Angkasa Pura I.
5. Meningkatkan kompetensi dan kapasitas sumber daya penanggulangan dan pemulihan keamanan siber di lingkungan PT. Angkasa Pura I.
   1. **Konstituen**

Konstituen AP1-CSIRT meliputi PT. Angkasa Pura I dan seluruh kantor cabang

* 1. **Sponsorship dan/atau Afiliasi**

Rencana Kerja dan Anggaran Perusahaan PT. Angkasa Pura I Republik Indonesia.

* 1. **Otoritas**

AP1-CSIRT merespon dan melaksanakan penanganan secara teknis terhadap insiden keamanan siber yang terjadi di lingkungan PT. Angkasa Pura I dan unit kerja dibawahnya.

1. **Kebijakan – Kebijakan**
   1. **Jenis-jenis Insiden dan Tingkat/*Level* Dukungan**

AP1-CSIRT memiliki kewenangan untuk menangani berbagai insiden keamanan siber yang terjadi atau yang mengancam konstituen AP1-CSIRT. Dukungan yang diberikan oleh AP1-CSIRT kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden.

* 1. **Kerja sama, Interaksi dan Pengungkapan Informasi/ data**

AP1-CSIRT akan menjalin kerja sama dan berbagi informasi dengan CSIRT/organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh AP1-CSIRT akan dirahasiakan.

* 1. **Komunikasi dan Autentikasi**

Untuk komunikasi biasa AP1-CSIRT dapat menggunakan alamat e-mail dan telepon. Namun, untuk komunikasi yang memuat informasi rahasia dapat menggunakan e-mail yang ter-enkripsi.

1. **Layanan** 
   1. **Layanan Utama**

Layanan utama dari AP1-CSIRT yaitu :

* + 1. **Pemberian Peringatan Terkait Keamanan Siber**

Layanan ini dilaksanakan oleh AP1-CSIRT berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik dan informasi statistik terkait layanan ini diberikan oleh AP1-CSIRT

* + 1. **Penanganan Insiden Siber**

Layanan ini merupakan layanan teknis terkait penanganan insiden yang terjadi pada konstituen yang meliputi koordinasi, analisis, rekomendasi teknis, dan bantuan on-site jika diperlukan, agar sebuah insiden tidak terulang kembali.

* 1. **Layanan Tambahan**

Layanan tambahan dari AP1-CSIRT yaitu :

* + 1. **Konsultasi terkait kesiapan penanganan insiden siber**

Layanan ini berupa konsultasi terkait kesiapan penanggulangan dan pemulihan insiden yang terjadi di lingkungan PT. Angkasa Pura I dan unit kerja dibawahnya.

* + 1. **Pembangunan kesadaran dan kepedulian terhadap keamanan siber**

Layanan ini berupa sosialisasi kepada konstituen AP1-CSIRT yang bertujuan untuk meningkatkan kesadaran dan kepedulian tentang keamanan informasi.

1. **Pelaporan Insiden**

Laporan insiden keamanan siber dapat di input oleh konstituen melalui aplikasi LAPORKAN INSIDEN pada website AP1-CSIRT atau dikirimkan ke alamat csirt[at]ap1.co.id dengan melampirkan :

1. Penjelasan insiden.
2. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan
3. Atau penjelasan tambahan lainnya.
4. ***Disclaimer***

Terkait penanganan jenis insiden, menyesuaikan tingkat dan dampak insiden serta ketersediaan perangkat dan sumberdaya yang dimiliki.