RFC 2350 CSIRT Mubadala Energy South Andaman (MESA – CSIRT)

1. Informasi Mengenai Dokumen

Dokumen ini berisi deskripsi CSIRT Mubadala Energy South Andaman (MESA – CSIRT) berdasarkan RFC 2350, yaitu informasi dasar mengenai CSIRT Mubadala Energy South Andaman (MESA – CSIRT), menjelaskan tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi CSIRT Mubadala Energy South Andaman (MESA – CSIRT).

1.1. Tanggal Update Terakhir

Dokumen ini adalah versi 1.0 yang diterbitkan pada tanggal 29 Agustus 2025.

1.2. Daftar Distribusi untuk Pemberitahuan

Dokumen ini didistribusikan kepada Badan Siber dan Sandi Negara (BSSN) dan pihak regulator terkait (misalnya SKK Migas), serta pimpinan internal yang membidangi keamanan siber.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia untuk diunduh pada situs resmi https://s.id/csirt-mesa

1.4. Keaslian Dokumen

Dokumen telah disahkan oleh manajemen berwenang di CSIRT Mubadala Energy Indonesia dan ditandatangani secara elektronik.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 CSIRT Mubadala Energy South Andaman (MESA – CSIRT);
Versi : 1.0
Tanggal Publikasi : 29 Agustus 2025;
Kedaluwarsa : Dokumen ini berlaku hingga ada dokumen RFC 2350 terbaru yang menggantikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Computer Security Incident Response Team (CSIRT) Mubadala Energy South Andaman
Disingkat : MESA-CSIRT

2.2. Alamat

Menara Astra, Lantai 18, Jl. Jenderal Sudirman Kav. 5-6, Jakarta Pusat 10220

2.3. Zona Waktu

WIB – Waktu Indonesia Barat (GMT+7)

2.4. Nomor Telepon

(+62 21) 39807200 (jam kerja Senin–Jum'at, 07.00–18.00 WIB)

2.5. Nomor Fax

02139807203

2.6. Telekomunikasi Lain

Tidak ada

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

id[dot]csirt[at]mubadalaenergy[dot]com

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

Blok PGP Public Key:

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

mQINBGjso60BEACkLGXzwXFwseFZ4WM7lk3UCOBffJDP/aP7tVNyc8gBGrJMGv/L
47hDdzt8BPh1A1HXqdDmbJjX7/JX2VkIvtIGifk/xHdiEN6J2o+0RBb67DhmwUWW
ajAXdqdVZzH3Mmn8AwSL1r3hw72wqODxzmLff5op5cYCWylQtISAAjze32jNV/NV
Slex/VeAYkFSrJ0MWTBWkucB8t/IDz0IglZQYxWxVNXC+YerfR34UE4c16C8P6IN
qaJ+MKMArCGq9U3lfpJIX6SlKkCF2mCDKVEU6DTInHTQkFSGYACjxuM23gZWOtUS
CDkrtFf4wWOQ1itkSW6MgIOVJj7aT7tRl+WoYIFpLPruGORvzubjQFIJdHrXRMKO
wysWXf9wDsjFDBvlTqgmv25Aj50NQUjT4fQqXSrbpgoKRLXUNkMhzfMXV9DBEC15
8eRL8+FTf3rXSaOU8BMNfs6hw92pE4ra1vF0tXDEadyj8GDkNkH8nNMlVl89krxB
4KmDib6bU7PtrB68i+dzB/3IBC9bqc7BCsUoVgDy8BEcDlndvUmncQCXNLuIklFw
8qTXOaoqrhhcFHpeEsJjSLlqOkhgFS5FCrKOwM+d02UV3BPQNm55BHRdg67l/tYs
3Gu3Cg+LONDck24hasEmQjz2fvi+xZ1KEs4ZPf+m1LNVuQVfRA0TFBFjTQARAQAB
tDhJRCBDU0lSVCAoTXViYWRhbGEgRW5lcmd5KSA8SWQuY3NpcnRAbXViYWRhbGFl
bmVyZ3kuY29tPokCVgQTAQgAQRYhBNbQW+MLGQHr2/nScKhNVNw6emaeBQJo7KOt
AhsDBQkJV2SjBQsJCAcCAiICBhUKCQgLAgQWAgMBAh4HAheAAAoJEKhNVNw6emae
fwEP+PPhcFanKeo0U5ZuvgIMvq+Z5KHD+/8jnuSh8zaP7OpeTSy9BNMmCG3ZZzc7
/km/8YxB/0+fUciokbktzpL8tne8LinvxjZBk0HY+I4Z8u/HPAW89MLcVk8fNzn2
FUD5+2BratobbFRLs6WFBCLut90eqjOinnbm0KyZ2cUSgssIH15Doeqpw+An0wTk
uUwWKTOd1tRzxPT5mNRC3XCe1p7VYK5cVwqNjVI0b+WVIhdphSIeGW95oSsjeZ0+
kUnhxDOLP1zSKuUJ8Lc9ze+vedXLpCN+gqBlrQpMMrgSzn3Jzhour9zR+5IcHSd+
woMGfhI5VDoOx+vtAlwRdtwCAf0WJhG47RhUWE9k8AvH6XtIfSjZ4nA/H/VteDzH
WhAHad4zKOnNaOHz7oQL3B/Dw4yQHgaVmMNur80xFcAms+0qfmA0egx0SrtzOiul
BCbfGlgA95xImyA+vv9hmdU1IulQ9a6a9drPRx0LA9611TJzEZJ1Lm/EBtQZPodn
O8X3yJaLcWmQiv0fFPwc71X+Q1O1PCoGrMqS9tHTG/4/oVzTA2PPzA9US2YBNxl2
N2jjf0AZesQ30VTANRzo3QWIf+ouxVxEnb3QtUm0UW7CUcmMlPB6ZRbd54J0huQd
g/jvMscqOT2Nxn5B5Lkck70OqTQ2U26oSb+79kVwwGCmx4y5Ag0EaOyjrQEQAOVV
vWftKaBzlMB99cAkmsazc6GtJsVwr4b47HqXoTopbWkraf02nCpKYpjjIoQ7+6+M
akKylPHxnd8q30XuFCzyitsxjldmzkcvBBcNRrRv7Qu0ueovHWHAxYNevl+Whqqb
ZJioWSfp9mRmt0ZBw8z4jP5F5kXNN9B3pUNd6hhCUjqXKC5N5pY9KJW4hU/wyBgx

3+E4aeLgK8ehCfcHP0Vn64j0Q8UEbZntdzb3gwmBhpry5I/iNJVbBb/hWeCYAhe9
OOKOZHOhbJUQqItXWBaJhi3gAN/696wEV4iMXtCqhYpg4sOJlmozCrqSkU9SGIIs
9X8VHkSv1yRlrGLP8vAERI22qRyp9bBRN+LgFcX2yhDnd/phrbTgMYrNPsrcCVD6
SWOb5pt6pRdSpmixlEJOsIwaaunLa6hz5U7kKxnMgFid+auCOPZnzrGXwM9OxpPC
MHfcQ1iMoxTOJJ+LyRw772sQp3EqhG6aufuJ6o1B0YAULLDLNVAHhltt2dAzGKhG
zbiydwu8nODhQ5gAN3b9J2vCOR7yo/rIcd+xCprMAE+OElqMIZ8UKXNYPZyDTI05
ueoh5ajizPej/naLQbi558y/+h5af1IUF1/C6/t7YZ79wcvNRC6eY0hJr182hjXU
0E5XnTw16430FSgSZqdTnoCAESisQbxu3A//boB7ABEBAAGJAjwEGAEIACYWIQTW
0FvjCxkB69v50nCoTVTcOnpmngUCaOyjrQIbDAUJCVdkowAKCRCoTVTcOnpmnm21
EACaRTiL+bvG/2y6WFPL4U+K5w0ojVAO+fHr51LB1aT0IkMI9j60BITqa1MZ4W1y
xKOdFZLNs98JNMqhZWqGnm5fAwpT/n9aqSfWNzZOf6bOuXNqn5Q4lzUzOZPLpBYc
Cau3I59lzgnidEqdxn3Te/qsLM37xlxkvARTEmTNgKdEGna1wYYr4XQWLfQJlut/
/03cV3Vj1lFpdqD4A2umZJ07Y0DFfpJP+Dg+oDWEvNGfx3jpo7zq7PO+RHuizjuc
RfXdsgTdV7HgF6raKv49SU52n5Hh6KCFFuUr2hxZmuZzixkSFGCJ+3H6VZUW3U9M
hbWsmQHo4gPnquZnL9KcdwCF4qq5UwEokkTjCKoag5faaCI7UvSuD45plwFiWuew
YJE1+RhjvOzYnOHPTPK5LetnXa+roXoLchhtr8rSqG/FxK2EL37QMUhN7QANFbqY
fiYFghC9DjGE30NOA3+GkAGFzBcgNJYtmB6wQssIPzrI3w0/fYBpqzXiN8LITMMp
Bkbgju3gv6tAPbL+qnAsfvI7/jOX40EcB7MGOnhyJqcxSX+cGO5Z89EY0d06Cn7M
qKcM+HAplNVM0GGLfHq/v7HUGhq8sEk/Z0ijg4S8wts7I5LLMEXXmfHd3LJx+Nni
dA8ZBP5GkYZvfixOgg/DMNwmuxaqEFoQeT7qK0h4/ODT2g==
=KFfc
-----END PGP PUBLIC KEY BLOCK-----

2.9. Anggota Tim

Ketua **CSIRT** adalah *Manager IT Indonesia*. Anggota tim mencakup perwakilan dari berbagai fungsi terkait keamanan siber perusahaan, antara lain:
Ketua: Manager IT Indonesia
Sekretaris: IT GRC Indonesia Lead
Manajer Krisis: HSSE & Asset Integrity Team Indonesia
Manajer Keamanan Siber: Manager Cybersecurity
Sub-tim Pusat Layanan Insiden TI: IT SOC Team
Sub-tim Komunikasi: Communication Team Indonesia
Sub-tim Hukum: Legal Team Indonesia
Sub-tim Pengelolaan Risiko: HSSE & Asset Integrity Team Indonesia
Sub-tim Keamanan Fisik: HSSE & Asset Integrity Team Indonesia

2.10. Informasi/Data lain

CSIRT ini tergolong **Tim Tanggap Insiden Siber Organisasi**. Seluruh pendanaan operasional CSIRT berasal dari anggaran internal perusahaan (pendanaan mandiri). Mubadala Energy South Andaman (MESA – CSIRT) juga merupakan bagian dari ekosistem keamanan siber perusahaan global, berkoordinasi dengan tim Global IT Security di kantor pusat sesuai arahan yang berlaku

2.11. Catatan-catatan pada Kontak MESA-CSIRT

Metode yang disarankan untuk menghubungi MESA-CSIRT adalah melalui e-mail pada alamat id[dot]csirt[at]mubadalaenergy[dot]com atau melalui nomor telepon ke

(+62 21) 39807200 (jam kerja Senin–Jum'at, 07.00–18.00 WIB) atau siaga selama 24/7.

3. **Mengenai** MESA-CSIRT

3.1. Visi

Visi MESA-CSIRT adalah menjadi tim tanggap insiden siber terdepan yang proaktif, andal, dan tepercaya dalam melindungi aset informasi Mubadala Energy, memastikan keberlangsungan operasional perusahaan, serta memperkuat kolaborasi dengan regulator nasional (BSSN dan SKK Migas) demi terciptanya ekosistem keamanan siber perusahaan yang tangguh dan berkelanjutan.

3.2. Misi

Misi dari MESA-CSIRT Tim Tanggap Insiden Siber (CSIRT) Mubadala Energy Indonesia berkomitmen untuk melindungi aset informasi perusahaan melalui penanganan insiden siber yang efektif, cepat, dan terkoordinasi, serta mendukung penerapan dan peningkatan berkelanjutan Information Security Management System (ISMS) sesuai standar ISO/IEC 27001.

3.3. Konstituen

Konstituen **MESA-CSIRT** meliputi seluruh unit bisnis Mubadala Energy di Indonesia (baik bidang IT maupun OT), termasuk kantor pusat Jakarta dan fasilitas operasi (shorebase Lhokseumawe), serta mitra atau kontraktor kritikal perusahaan. Dengan demikian, seluruh entitas internal perusahaan dan pihak eksternal terkait layanan TI perusahaan yang berada di Indonesia masuk dalam cakupan layanan CSIRT ini.

3.4. Sponsorship dan/atau Afiliasi

CSIRT ini merupakan bagian integral dari organisasi Mubadala Energy South Andaman RCS Ltd (Indonesia), sehingga seluruh dukungan pendanaan berasal dari perusahaan (didanai secara mandiri oleh Mubadala Energy). CSIRT berafiliasi dan berkoordinasi dengan tim keamanan siber perusahaan sesuai kebijakan internal, serta tunduk pada arahan regulator sektor (SKK Migas) sebagaimana diperlukan.

3.5. Otoritas

MESA-CSIRT memperoleh otoritas melalui Surat Keputusan Manajemen yang mengacu pada regulasi nasional serta kebijakan internal perusahaan. Otoritas ini memberikan mandat kepada CSIRT untuk bertindak secara operasional dalam penanganan insiden siber di seluruh unit bisnis dan lingkungan kerja perusahaan, termasuk mitra kerja terkait. Dalam pelaksanaannya, CSIRT berwenang melakukan pemantauan keamanan, respons insiden, koordinasi mitigasi/pemulihan, hingga pelaporan insiden secara terintegrasi. Hubungan antara otoritas CSIRT dan konstituen tercermin dari cakupan layanan tim yang mencakup deteksi dini, penanggulangan, dan penanganan insiden bagi seluruh konstituen, sesuai standar ISO/IEC 27001:2022 serta arahan BSSN dan SKK Migas yang relevan.

4. Kebijakan – Kebijakan

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

MESA-CSIRT menangani berbagai jenis insiden siber yang mengancam konstituen, termasuk (namun tidak terbatas pada) insiden terhadap sistem Teknologi Informasi maupun Teknologi Operasional perusahaan. Contoh jenis insiden meliputi: malware, phishing, peretasan website (defacement), Distributed Denial of Service (DDoS), dan insiden lainnya yang berdampak pada kerahasiaan, integritas, atau ketersediaan layanan informasi perusahaan. Dukungan yang diberikan oleh CSIRT kepada konstituen akan disesuaikan dengan jenis dan tingkat keparahan insiden.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

MESA-CSIRT aktif menjalin kerja sama dan koordinasi dengan lembaga eksternal seperti BSSN serta CSIRT lainnya dalam rangka mendukung upaya keamanan siber nasional. CSIRT siap berbagi informasi seputar insiden siber dengan instansi pemerintah (pusat maupun daerah), regulator, penegak hukum, maupun konstituen terkait, terutama jika kolaborasi tersebut diperlukan untuk penanganan insiden yang melibatkan berbagai pihak. Dalam berbagi informasi dan berinteraksi, CSIRT menjaga kerahasiaan data sesuai peraturan – informasi sensitif yang diterima oleh CSIRT (termasuk rahasia negara, rahasia perusahaan, maupun data pribadi) akan dijaga kerahasiaannya dan hanya diungkapkan kepada pihak berwenang atau konstituen yang membutuhkan saja. Kebijakan internal mengatur bahwa informasi insiden yang bersifat rahasia tidak akan dipublikasikan tanpa izin.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi **biasa/rutin**, **MESA-CSIRT** menggunakan sarana email dan telepon resmi tim sebagai media utama. Komunikasi instruksional atau notifikasi insiden disampaikan melalui email *id[dot]csirt[at]mubadalaenergy[dot]com* dan jika diperlukan, melalui telepon kepada kontak yang ditunjuk. Dalam hal pertukaran informasi sensitif atau terklasifikasi, CSIRT menerapkan mekanisme autentikasi tambahan dan jalur komunikasi **terenkripsi/aman**. Misalnya, sebelum berbagi informasi sensitif, identitas pihak yang berkomunikasi akan diverifikasi, dan bila tersedia, enkripsi (misalnya menggunakan **PGP/GPG**) akan digunakan untuk melindungi kerahasiaan pesan.

5. Layanan

5.1. Layanan Utama

Layanan utama dari **MESA-CSIRT** yaitu :

Layanan Utama	Deskripsi
Pemberian Peringatan Terkait Keamanan Siber	Layanan berupa penyampaian *alert* dan peringatan dini mengenai kerentanan atau ancaman siber terbaru kepada konstituen. CSIRT akan menginformasikan adanya insiden atau ancaman (misalnya malware baru, ancaman *zero-day*, indikasi serangan) kepada pemilik sistem elektronik terkait, termasuk memberikan saran tindakan pencegahan yang perlu dilakukan. Peringatan ini membantu konstituen

	mengambil langkah proaktif sebelum insiden berdampak lebih luas.
Penanganan Insiden Siber	Layanan berupa respons terhadap insiden siber yang terjadi, mencakup koordinasi, analisa, rekomendasi teknis, hingga bantuan langsung (*on-site*) untuk penanggulangan dan pemulihan insiden. CSIRT akan berperan sebagai pusat kendali insiden: menerima laporan insiden, melakukan analisis awal, memberikan panduan mitigasi kepada tim teknis/pemilik sistem, membantu isolasi/penyelesaian masalah, serta memastikan langkah pemulihan sistem berjalan hingga tuntas. Jika diperlukan, CSIRT akan turun langsung bersama tim teknis terkait untuk menangani insiden kritis.

5.2. Layanan Tambahan

Layanan tambahan dari **MESA-CSIRT** yaitu :

Layanan Tambahan	Deskripsi
Penanganan Kerawanan Sistem Elektronik	CSIRT menerima dan menindaklanjuti laporan kerentanan (vulnerability) pada sistem elektronik milik konstituen. Layanan ini mencakup analisis kerawanan yang dilaporkan, koordinasi dengan pemilik sistem untuk verifikasi, serta rekomendasi tindakan perbaikan atau patch. Apabila kerentanan ditemukan melalui audit internal ataupun laporan pihak eksternal, CSIRT membantu memastikan bahwa kelemahan keamanan tersebut ditangani secara tuntas (misalnya melalui pembaruan sistem) demi mencegah eksploitasi oleh pihak yang tidak berwenang.
Penanganan Artefak Digital	Layanan analisis terhadap artefak digital yang terkait insiden, misalnya berkas mencurigakan, malware, atau bukti digital lainnya. CSIRT akan menganalisis artefak tersebut untuk mengidentifikasi sifat ancaman (contoh: melakukan analisa malware), memberikan informasi teknis tentang artefak, dan mendukung proses forensik jika diperlukan. Hasil analisis artefak ini membantu pemulihan sistem yang terdampak insiden serta dapat menjadi masukan dalam investigasi insiden lebih lanjut.
Pemberitahuan Hasil Pengamatan Potensi Ancaman	CSIRT secara proaktif memantau potensi ancaman siber yang relevan dengan lingkungan perusahaan. Layanan ini berupa penyampaian informasi atau laporan berkala kepada konstituen mengenai hasil pemantauan tersebut – misalnya tren serangan terbaru, kerawanan umum di sektor energi, atau informasi intelijen ancaman. Tujuannya agar seluruh pengguna dan unit bisnis waspada serta

	dapat mengambil langkah pencegahan sebelum ancaman berkembang menjadi insiden.
Pendeteksian Serangan	Layanan deteksi dini serangan siber melalui fasilitas pemantauan keamanan. CSIRT bekerja sama dengan **Security Operations Center (SOC)** atau penyedia layanan pemantauan (*Managed Security Service Provider/MSSP*) untuk memonitor jaringan dan sistem perusahaan selama 24/7. Apabila terdeteksi aktivitas anomali atau indikasi serangan (misalnya melalui sistem IDS/IPS atau firewall), CSIRT akan segera melakukan triase insiden dan menginformasikan tim terkait untuk langkah mitigasi cepat. Dengan deteksi serangan ini, banyak insiden dapat dicegah atau dampaknya diminimalkan sedini mungkin.
Analisis Risiko Keamanan Siber	CSIRT melakukan penilaian dan analisis risiko keamanan siber terhadap aset informasi dan infrastruktur TI perusahaan. Berdasarkan data insiden yang pernah terjadi, kerentanan yang ditemukan, serta intelijen ancaman, CSIRT mengidentifikasi skenario risiko potensial dan tingkat paparannya terhadap bisnis. Laporan analisis risiko ini membantu manajemen dalam memahami prioritas keamanan yang perlu ditingkatkan dan menyusun rencana mitigasi untuk mengurangi risiko siber secara proaktif.
Konsultasi Terkait Kesiapan Penanganan Insiden Siber	Layanan konsultasi bagi konstituen mengenai kesiapan dan kapabilitas menghadapi insiden siber. CSIRT menyediakan bimbingan atau saran tentang prosedur tanggap insiden, pembuatan rencana respon insiden, pengujian (drill) insidentil, serta peningkatan kompetensi tim teknis konstituen. Melalui konsultasi ini, CSIRT membantu unit-unit bisnis memastikan bahwa mereka memiliki rencana dan kesiapan yang memadai untuk merespons insiden (sejalan dengan kerangka Business Continuity/Disaster Recovery yang ada). Konsultasi dapat berupa sesi pelatihan singkat, workshop, atau evaluasi kesenjangan (gap assessment) terhadap prosedur penanganan insiden di unit tersebut.
Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber	CSIRT menjalankan program-program *security awareness* untuk menumbuhkan kesadaran keamanan siber di kalangan karyawan/konstituen. Layanan ini dapat berupa sosialisasi, kampanye, atau pelatihan berkala tentang praktik keamanan informasi yang baik, simulasi phishing untuk edukasi, penyebaran materi edukatif, dan sebagainya. Tujuannya agar seluruh konstituen memahami pentingnya melindungi informasi, mengenali ancaman siber umum, serta mengetahui peran dan

	tanggung jawab masing-masing dalam menjaga keamanan siber perusahaan.

6. Pelaporan Insiden

Setiap insiden keamanan siber yang dialami konstituen dapat dilaporkan kepada CSIRT agar dapat ditangani. Laporan insiden keamanan siber dapat dikirimkan melalui email ke id[dot]csirt[at]mubadalaenergy[dot]com dengan melampirkan sekurang-kurangnya :

a. Foto/*scan* kartu identitas
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan
c. Informasi tambahan sesuai ketentuan lain yang berlaku (misalnya kronologi singkat, dampak yang dirasakan, kontak yang dapat dihubungi untuk koordinasi lanjutan)

CSIRT akan menindaklanjuti laporan insiden yang masuk sesuai prosedur. Pelapor diharapkan memberikan informasi selengkap mungkin agar membantu proses analisis insiden. Seluruh laporan yang diterima akan dicatat dalam sistem pencatatan insiden CSIRT dan akan dijaga kerahasiaannya. Jika diperlukan informasi tambahan, CSIRT akan menghubungi pelapor melalui kontak yang disediakan.

7. *Disclaimer*

Informasi yang bersifat operasional dan teknis dalam dokumen ini tunduk pada ketentuan kerahasiaan dan regulasi yang berlaku. Penyebarluasan atau penggunaan dokumen ini di luar tujuan resmi harus mendapatkan persetujuan tertulis dari MESA-CSIRT.