RFC 2350 *MMP-CSIRT*

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 13 Maret 2026.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan pembaharuan dokumen.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :

https://docs.google.com/document/d/1kZ2UMN-qKYn_CWBoJBDXSNrLKfH1ZCGs/edit?usp=drive_link&ouid=105644814834507767585&rtpof=true&sd=true

(versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Dokumen telah ditanda tangani oleh Ketua *MMP-CSIRT*. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 *MMP-CSIRT*;
Versi : 1.0;
Tanggal Publikasi : *13 Maret 2026*;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

PT. Mega Marine Pride – Computer Security Incident Response Team
Disingkat : *MMP-CSIRT*.

2.2. Alamat

Wonokoyo, Purwodadi, Gunungsari, Kec. Beji, Pasuruan, Jawa Timur 67154

2.3. Zona Waktu

Indonesia (GMT+7)

2.4. Nomor Telepon

(0343) 656446

2.5. Nomor Fax

N/A.

2.6. Telekomunikasi Lain

N/A.

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

csirt@megamarinepride.com

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

KEY ID	: 0x9E280985B686520A
Algorithm	: RSA
Length	: 3072
Fingerprint	: 3873 505F DB8E 3ED1 5810 A0ED 9E28 0985 B686 520A
Created	: 3/5/2026
Expiry	: 3/4/2031

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

xsDNBGmpJqIBDADhI/cRUIdK7L7x66UcMmuf544CMtiby5H3z9fmdnJ2H5wIOvwp
+epa//MA1mJbjnGfVhle2eLv1/Zv8MA/ahBMsxe703lvEK1xq2nI57J3LqLPCBqQ
wrCHCqBTsiAUBDUNTq4G+U/qAbIGOEQEkpsZxUl4S7Wln6WDLGsDeaGUceHw402Y
lQfm48wSoqRFKJQpgpaNCvuEKwsdR4t2vfc10EGALVq9IwgwbsTuZB4Rts5CbS2d
RMM32U1yFzLzLiWmtP0SdWxMdVAU9SUHxcw2rsueCNpjqym1NdB9uFonfpS153Hr
znZthZXdabIM/9PYLA+CyfB4Q7YNXaRuElfsMEikUNgYUXAZ1bOCxV+ssMiuFkXL
9yXcuAHRwPN4KJUflFMZZ4ViN21qhImUqjhPibq5EHpzrALTLLP3ZISe8VSaoCpv
cEm14FlkiF1OsLm+RtzBBDrpJRlWJN8T80eTrY0amJz7/Dh6ti30zaS31sBXpyMv
FUmt4dz+O8UHmbsAEQEAAc0lTU1QLUNTSVJUIDxjc2lydEBtZWdhbWFyaW5lcHJp
ZGUuY29tPsLBDQQTAQgANxYhBDhzUF/bjj7RWBCg7Z4oCYW2hlIKBQJpqSajBQkJ
ZgGAAhsDBAsJCAcFFQgJCgsFFgIDAQAACgkQnigJhbaGUgqlBQv9Fe41s1yJ0F91
+VwmxgV0hwcLyIlfZ0A6DYIaVy4Bw9SvPJ7Dhs+3+ibOq4dhd83tb6HVLs2/QIMo
TlkWdTQKL3oneevBun90FlKYqRnfj+UMbfdREnikXeZSkM8Z42vUljxWtEoJ0EZQ
OdETyHmA4ApUJORr45Nk+B2TpCRyD7wDSwTYwNqwoBmYnlp7cTyyxlPOrBpJ8gya
dQcCQN54M8QwWP2PPp+kTlCg70UwYU9fccQrqc0OITfqOi7t9eEqau+f+hFpHOH+
+ZIKPke3MxOtzAU/1f4S/lLZXbfWi2On3196LrBdFJEMSbxMuNJvHCy7eCrRzmk5
J2eVLSsNaQ4+8a6tZmZyRx3h+lONGQ2RdiKHqTlOzz5A7SHmRQIiC0ToOjfhRoL7
qA9pn4ziYDU2pmDuFI4BuA3AJFA7lTxKd/u2a17vJ7NbWNUZuHUVC4U976gMAB23
/bNUWRRGr5Vx3FwGp34SMCeFzhaQQDNMa8GytM84CrJZ6cB0CPajzsDNBGmpJqMB
DADsc7SwlfLrVjUFwUYVzua8OT27Evts0eN2NEmAdbdd57QvIQfV0Cs4YgN8fo3B
6cMi0aq9IphUZvXhPSRs1OPProTmjq3Zapl4UJPiwnuzXW4Z72WLesT3DlaJs368
0zKIEwp1YZoLxtbghVvD4U+A3N2wjTbJFuJWhbHFP6rTtb6oSz9LZ+8xTOny2f7v
6J0oBRNE2HnbwP2UBziSLTnPCIF4jCiISWWQJf/EsqUoDnZ6qifFifW7drqwQCjo
CLuaTiFMZNboyvLT813zUuFKZnAPNaIMsOok0WTNDiCJEOC/JRQH5+4B5RmkbfzZ

OKGNVF8e/tljZgPetQzE2CmVQouZJNBqjj34Meuly6ysji5m3OjGfUNoAefVgjjq
MBgq1D0ihCeHrB+WDBctY/eDy2fvX56IGds+yAm3nECd7QHPrMbavXhTwYhVTh89
dqlPGwdGw8vKLHFU1vNTKe3F9ipHKopxfL+CWThMGYsTltuUoAD1YUAtY5tTVzgW
B0cAEQEAAcLA/AQYAQgAJhYhBDhzUF/bjj7RWBCg7Z4oCYW2hlIKBQJpqSajBQkJ
ZgGAAhsMAAoJEJ4oCYW2hlIKDL8MAIjRx3lANO3JC2y+JY3MJNhK2TxEDjRXxPeE
6vcfDAr2ieylIYtLTkEvo6e6ShU80o3B+dZ4wy4XPiG6f8Og+zfXHlCiRiX/I3aV
2HktfNAkq81vQeUvGOtLoTgzdKR5QIIRNPsM+Brg8gJ6rEWdnrntyBA5W4Ux3QEN
lakkGKM/D0kOmpcJoSs0aNQeTngV2I60ma32lTQqthfvSOvwXK3ofzOY+bRcBfkn
WtZ+2XJmwuoOs+ameAl5aAuuEQYvsrsyWl0Q5VPeD6CZo5N6PvFY9QT6g8+8/8kV
T2odnkmJEc0YV6OmaTEqIcOncG+fOxIyYVb2MlwPKsTqxGuDgkSG+T6Q2qygMN4M
l7h+bBoYuz8P58dr+p0jKPF66U2Oej/FB7xZTWijKBzhnXr8vYr5WwMFb5VAMxOv
TGejPyJkCLaJlxF/JjBs6VJKbSBy09keDjNHfuwBgTBrBkevBZFy+LOASj/NtbwZ
jwzff/5XeS3VlIJX+czLRUztudN2Q==
=4E6i
-----END PGP PUBLIC KEY BLOCK-----

File PGP key ini tersedia pada:
https://docs.google.com/document/d/11WDNH5kQIZJjAem1zfnav_fX0uxsJLaVOUaDfmCpydE/edit?usp=drive_link

2.9. Anggota Tim

Ketua *MMP-CSIRT* adalah IT Manager PT. Mega Marine Pride.
Yang termasuk anggota tim adalah tim IT PT. Mega Marine Pride.

2.10. Informasi/Data lain

N/A.

2.11. Catatan-catatan pada Kontak MMP-*CSIRT*

Metode yang disarankan untuk menghubungi *MMP-CSIRT* adalah melalui *e-mail* pada alamat csirt@megamarinepride.com atau melalui nomor telepon yang tercantum pada Informasi Data/Kontak. Pada hari Senin-Jumat pada pukul 08.00-17.00 WIB dan jika terdapat hal-hal yang mendesak di luar jam tersebut dapat dilakukan penanganan.

3. Mengenai *MMP-CSIRT*

3.1. Visi

Visi *MMP-CSIRT* adalah menjadi komponen utama untuk tercapainya Visi Perusahaan dengan meningkatkan ketahanan siber serta memastikan keamanan dan keberlangsungan operasional Perusahaan.

3.2. Misi

Perwujudan visi sebagaimana dituangkan di atas akan dicapai melalui upaya-upaya yang terkandung dalam misi *MMP-CSIRT*, yaitu :

a. Mengkoordinasikan dan mengkolaborasikan layanan keamanan siber di lingkungan Perusahaan dan pemangku kepentingan terkait.
b. Membangun kemampuan dan kapasitas sumber daya keamanan siber di lingkungan Perusahaan.

c. Membangun kerjasama dalam rangka penanggulangan dan pemulihan insiden keamanan siber di lingkungan Perusahaan.

3.3. Konstituen

Konstituen *MMP-CSIRT* meliputi seluruh pengguna yang menggunakan layanan teknologi informasi di PT. Mega Marine Pride, meliputi karyawan dan anak perusahaan, yaitu PT. Baramuda Bahari

3.4. Sponsorship dan/atau Afiliasi

Pendanaan *MMP-CSIRT* bersumber dari anggaran unit kerja terkait.

3.5. Otoritas

Berdasarkan Kebijakan Pengelolaan Sistem dan Teknologi Informasi dan Kebijakan Pengelolaan Keamanan Informasi, *MMP-CSIRT* memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi, dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber yang terjadi di konstituen.

4. Kebijakan – Kebijakan

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

MMP-CSIRT memiliki otoritas untuk menangani insiden yaitu :

a. Web Defacement;
b. DDOS;
c. Malware;
d. Phising;

Dukungan yang diberikan oleh *MMP-CSIRT* kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

MMP-CSIRT akan melakukan kerjasama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh *MMP-CSIRT* Indonesia akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa *MMP-CSIRT* Indonesia dapat menggunakan alamat e-mail tanpa enkripsi data (e-mail konvensional) dan telepon. Namun, untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi PGP pada e-mail.

5. Layanan

5.1. Layanan Utama

Layanan utama dari *MMP-CSIRT* yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

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

5.1.2. Penanganan Insiden Siber

Layanan ini diberikan berupa kegiatan menerima, menanggapi, dan menganalisis Insiden Siber.

5.2. Layanan Tambahan

Layanan tambahan dari *MMP-CSIRT* yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini berupa koordinasi, analisis dan rekomendasi teknis dalam rangka penguatan aspek kendali keamanan (security control) baik dalam lingkup teknis ataupun non-teknis (Policy/Governance).

Secara umum penanganan ini dibagi menjadi :

1. Pelaporan kerawanan yang bersifat sewaktu oleh pemilik/penyelenggara sistem elektronik milik konstituen.
2. Layanan penanganan kerawanan sebagai tindak lanjut dari kegiatan audit atau vulnerability assessment

5.2.2. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini diberikan berupa penyampaian kepada konstituen terkait ancaman terhadap Sistem Elektronik yang dapat muncul akibat perkembangan teknologi, politik, ekonomi, dan perkembangan lainnya.

5.2.3. Pendeteksian Serangan

Tim *MMP-CSIRT* memiliki beberapa sistem untuk mendeteksi apakah sistem pada perusahaan yang bersangkutan dengan stakeholder aman atau memiliki risiko, sehingga dapat dilakukan penanggulangan sedini mungkin.

5.2.4. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Tim *MMP-CSIRT* melakukan webinar mengenai isu sistem keamanan informasi.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt@megamarinepride.com dengan melampirkan Formulir Aduan Insiden Siber yang sekurang-kurangnya memuat :

a. Identitas Pelapor;
b. Tipe Laporan;
c. Waktu Terjadinya Insiden;
d. Tipe Insiden;
e. Deskripsi Insiden disertai Bukti (screenshoot, domain name, URL, email dll).
f. Atau sesuai dengan ketentuan lain yang berlaku

7. *Disclaimer*

Tim *MMP-CSIRT* memiliki beberapa tools untuk menghindari malware antara lain :

a. Menentukan asesmen tingkat keamanan informasi pada proses bisnis yang sedang atau yang akan berlangsung;
b. Melakukan asesmen tingkat keamanan sistem informasi yang dibuat secara sendiri (in-house), atau disewa/dibeli ke pihak ketiga;
c. Melakukan pengawasan serta intervensi aktif terhadap operasional sistem informasi dalam rangka pemenuhan ketahanan dan keandalan siber yang menunjang tujuan bisnis;
d. Merencanakan, membuat dan mengoperasikan rancang bangun mekanisme pertahanan berlapis siber (cyber defense-in-depth);
e. Melaksanakan program kesadaran keamanan siber bersama stakeholder terkait
f. Memiliki otoritas penuh untuk melaksanakan koordinasi dan intervensi internal dan eksternal, akses terhadap data dan sistem dalam hal penanganan insiden siber Anti – Malware.

Ketua MMP-CSIRT

Ismarwanto