

RFC 2350 Bank Maybank Indonesia-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.2 yang diterbitkan pada tanggal 19 Agustus 2025.

1.2. Daftar Distribusi untuk Pemberitahuan

Distribusi dokumen RFC dibatasi hanya untuk internal Bank Maybank Indonesia melalui media komunikasi internal.

1.3. Lokasi Dimana Dokumen Ini Bisa Didapat

Dokumen ini tersedia pada <https://www.maybank.co.id/others/rfc-2350>

1.4. Keaslian Dokumen

Dokumen ini telah ditanda tangani oleh pimpinan Bank Maybank Indonesia-CSIRT.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 Bank Maybank Indonesia-CSIRT;

Versi : 1.2;

Tanggal Publikasi : 19 Agustus 2025;

Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Bank Maybank Indonesia-Computer Security Incident Response Team

Disingkat : Bank Maybank Indonesia-CSIRT.

2.2. Alamat

Gedung Sentral Senayan 3, Jl. Asia Afrika No. 8, Senayan, RT.1/RW.3, Gelora, Jakarta Selatan, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10270.

2.3. Zona Waktu

Jakarta (GMT +07:00)

2.4. Nomor Telepon

021-29228800

2.5. Nomor Fax

-

2.6. Telekomunikasi Lain

-

2.7. Alamat Surat Elektronik (E-mail)

Alamat e-mail utama: csirt@maybank.co.id

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

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

mQENBGfRe/ABCAC0MwprtpM7wIYApuWtz1/bELS2hV7InkIRZgZJHz4Hv/n5G7IS
T8JJ8cmWeQqeQqyZKKbM8rAr0nhYJvodBNQj7yeH5r7jR4IP2IsCk2DfvDtfYYdO
EF3X84cerVTqnEiVNn2HbYdeJLkFjCicguWIHYs/BcMyoZquyOZSklyk00oCLHJm
VAbAtngcKzQUIZfOAG8wwyxCA0KJ9UEfUaUw/onGaUnQhNLanZmpCCmQpKQ29IM
r
mcqElRmgHsKwiCcGibdSM0Yjtc0oq8uFLVDUq8KSXcH2ilb8f0Nj0t+Z8FtEp3Ek

Llj53vvgzMegLxV7p2mn9cAFSB2g8rHe6xqXABEBAAG0H0NTSVJUIEICSSA8Q1NJ
UIRabWF5YmFuay5jby5pZD6JAVcEEWEIAEEWlQQLsjRARM0ISzK7CDtVbH5rWYks
0wUCZ9F78AibAwUJBaSE4AULCQgHAGliAgYVCgkICwIEFgIDAQleBwIXgAAKCRBV
bH5rWYks04KZB/9ZLiA1I5NXiM8aUnEzZ8yXhN5yVfr9kSrTWuRdyCvx25kAAh3y
2tkFh0toZ4T0p7ZflqBsgVUXTkWOBLyUxNgQYFIEGttfOcsC2CXQgX+r0GOKOb
nupl4Qj7ponupnBXFMmqdoBRUaBVfa2D6cXjAAXq4GdRrezHePHaQoFyJl+HCU/z
hUwYhznSCmn5Wl2st4Z9J2ptONDvAY8KmlTj3tw/B4QVm3zZOml9vn/ojsuhw6QN
PZNIlni8xpjiuhs0WDFIHnMZ6OdleESyULXSKZRmZZVqM9MDutiAN4/xBUI7Z8cXT
EIVNg66hk53u59WmeAlqXBrfUeDgJoed6W30uQENBGfRe/ABCADNV6XlFQd+edi
svo2M3VvxI5fU52fmNsJuJW3vog2BoTVTjJeMyeUnVXjxLimxVSv+dVtC5FqD8Qf
IZEI2QRMZFQhKzafn7kWI9SXyMZ9hVm/4IVsE6WQSJvFPNYI1Gjfr57fTuK/a8x6
WEVjK9xBGWJJgvfqScNsBS06nwA0xLKg49Wh4Jze5uIKCqJ8IKDU0CBnxQM0EoQ9
2JWzJbv+p8kiCH/oR7N0GnX3v+eLUC9DCIxAH/oSxtHHI2w4qewVfPStyzQsZtmi
V56hBbtcu+hBA0pXrbGWPQ1cujtl6ybT6HA6Y1QeyMzuNyEW/8Y0pGL78yLpt5ql
ql+fJqf5ABEBAAGJATwEGAEIACYWIQQLsjRARM0ISzK7CDtVbH5rWYks0wUCZ9F7
8AibDAUJBaSE4AAKCRBVbH5rWYks0IE4CAChruwXmyG0reyrpFRX6xRP5u7IN0M/
XNkxrEUysBJ6LbDGytiraqd7fv0w17uEROxT9ohludMyv8CLdmoBQzwh4V6Mo5x
t0PwTIsAG2NzWkJM8qAMJSwIBpMoytS3nhGmlvHikzEmLGmVCZIAwO5S6AM7Lh5p
FrOASMq+wj6n10SmrSXeiixIFJNxGqdxBOB9wUK7cb4H37NyM9Yulmvv/sCx9zRv
qPciYEZZi+GeG2eRIKTCUGFcsgvOr0lz3DRy8YALKC3X0GDafG9NA4y7pW9ul7tT
Msw99E4sEZgok+vjoQkuD+OhQrIk/W7dQPY0zxjxLW4PO1x2toxL/3v4
=L9+n
-----END PGP PUBLIC KEY BLOCK-----

2.9. Anggota Tim

Ketua/pimpinan Bank Maybank Indonesia-CSIRT adalah *Chief Information Security Officer* (CISO) yang bertanggung jawab memberikan arahan kepada seluruh *stakeholder* CSIRT bekerja sama dengan *Computer Security Incident Coordinator* (CSIC) yang dijabat oleh pimpinan unit kerja *IT Security*. Untuk susunan CSIRT dan anggota tim CSIRT merujuk kepada Peraturan Direksi Bank Maybank Indonesia NO.PER.DIR.2025.005/DIR IT & DIGITAL tentang Pengelolaan

Insiden Keamanan Teknologi Informasi tentang struktur *Computer Security Incident Response Team* (CSIRT).

2.10. Informasi/Data lain

Tidak ada

2.11. Catatan-catatan pada Kontak Bank Maybank Indonesia-CSIRT

Metode yang disarankan untuk menghubungi Bank Maybank Indonesia-CSIRT adalah melalui *e-mail* pada alamat csirt@maybank.co.id

3. Mengenai Bank Maybank Indonesia-CSIRT

3.1. Visi

Visi Bank Maybank Indonesia-CSIRT adalah terwujudnya ketahanan siber yang andal dan profesional di lingkungan Bank Maybank Indonesia.

3.2. Misi

Misi dari Bank Maybank Indonesia-CSIRT, yaitu :

- a. Membangun kapasitas dan kapabilitas sumber daya keamanan siber.
- b. Menyediakan sistem pengamanan yang mencakup prosedur dan sistem pencegahan, penanggulangan, dan pemulihan terhadap ancaman siber.
- c. Menyediakan mekanisme penanggulangan insiden dan/atau pemulihan insiden yang dilakukan oleh tim penanggulangan dan pemulihan insiden siber.

3.3. Konstituen

Konstituen Bank Maybank Indonesia-CSIRT meliputi seluruh unit kerja di lingkungan Bank Maybank Indonesia.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan BANK Maybank Indonesia-CSIRT bersumber dari anggaran perusahaan.

3.5. Otoritas

Bank Maybank Indonesia-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber pada organisasi Bank Maybank Indonesia.

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/Level Dukungan

Dukungan yang diberikan oleh Bank Maybank Indonesia-CSIRT kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden seperti dibawah ini namun tidak terbatas pada:

- a. *Denial Of Services (DOS) / Distributed Denial Of Services (DDOS)*
- b. *Malware*
- c. *Phishing*
- d. *Compromised Information*
- e. *Unauthorized Activity*
- f. *Compromised Asset*

4.2. Kerja Sama, Interaksi dan Pengungkapan Informasi/Data

Bank Maybank Indonesia-CSIRT akan melakukan kerja sama dan berbagi informasi dengan tim CSIRT/TTIS atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diberikan dan diterima oleh Bank Maybank Indonesia-CSIRT harus dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, Bank Maybank Indonesia-CSIRT dapat menggunakan alamat *email* tanpa enkripsi data (*email* konvensional) dan telepon. Namun, untuk

komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi pada *email*, data atau jalur komunikasi lainnya.

5. Layanan

5.1. Layanan Utama

Layanan utama dari Bank Maybank Indonesia-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini dilaksanakan oleh Bank Maybank Indonesia-CSIRT berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik dan informasi statistik terkait.

5.1.2. Penanganan Insiden Siber

Layanan ini dilaksanakan oleh Bank Maybank Indonesia-CSIRT berupa koordinasi, analisis, rekomendasi teknis, dalam rangka penanggulangan dan pemulihan insiden siber.

5.2. Layanan Tambahan

Layanan tambahan dari Bank Maybank Indonesia-CSIRT yaitu :

5.2.1. Penanganan Kerawanan/Kerentanan Sistem Elektronik

Bank Maybank Indonesia-CSIRT melaksanakan koordinasi, analisis, dan/atau rekomendasi teknis dilakukan secara periodik dalam rangka penguatan keamanan sistem informasi.

5.2.2. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini dilaksanakan oleh Bank Maybank Indonesia-CSIRT berupa *monitoring* secara berkala atas aset milik Bank Maybank Indonesia terhadap adanya potensi ancaman siber.

5.2.3. Pendeteksian Serangan

Menganalisa data untuk mendeteksi adanya serangan terhadap sistem elektronik atau aktivitas yang mencurigakan terhadap sistem elektronik atau pelanggaran terhadap kebijakan keamanan siber.

5.2.4. Analisis Risiko Keamanan Siber

Mengidentifikasi dan menilai risiko keamanan siber serta merekomendasikan tindak lanjut untuk menghadapi risiko tersebut.

5.2.5. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Memberikan wawasan, pemahaman, dan cara yang perlu dilaksanakan dalam rangka membantu penanganan insiden siber.

5.2.6. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Melaksanakan kegiatan meningkatkan kesadaran dan kepedulian pengguna sistem informasi terhadap keamanan sistem/siber dengan cara sosialisasi/pelatihan kepada Konstituen terkait di Bank Mandiri Taspen.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt@maybank.co.id dengan melampirkan sekurang-kurangnya :

- a. Foto/*scan* kartu identitas
- b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan
- c. Atau sesuai dengan ketentuan lain yang berlaku

7. Disclaimer

- Seluruh penanganan insiden siber bergantung pada ketersediaan *tools* dan sumber daya terkait yang dimiliki oleh Bank Maybank Indonesia-CSIRT.
- Waktu penyelesaian insiden siber bervariasi sesuai dengan kondisi situasional terhadap insiden yang dihadapi.