BADAN PENYELENGGARA JAMINAN PRODUK HALAL
PUSAT DATA DAN INFORMASI
Jl. Raya Pondok Gede Pinang Ranti No. 13 Makasar, Jakarta Timur 13560
Telp. 021 80877955 Website: www.bpjph.halal.go.id

RFC 2350 BPJPH-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.1 yang diterbitkan pada tanggal 13 Oktober 2025

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://bpjph.halal.go.id/bpjph-csirt/

1.4. Keaslian Dokumen

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikat Elektronik (BSrE), Badan Siber dan Sandi Negara.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 BPJPH-CSIRT;
Versi : 1.1;
Tanggal Publikasi : 13 Oktober 2025;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan

2. Informasi Data/Kontak

2.1. Nama Tim

Badan Penyelenggara Jaminan Produk Halal-Computer Security Incident Response Team (CSIRT)
Disingkat : BPJPH-CSIRT.

2.2. Alamat

Jl. Raya Pd. Gede No.13, RT.1/RW.1, Pinang Ranti, Kec. Makasar, Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta 13560

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

Telepon 176
Whatsapp Layanan BPJPH : 0811-1421-142

2.5. Nomor Fax

-

2.6. Telekomunikasi Lain

Email : csirt@halal.go.id

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

csirt[at]halal[dot]go[dot]id

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

Bits : 4096
ID : E088 17D1 EC94 75DA
Key Fingerprint : EA107A01262C56E7C4A9A8CAFF374C08D9B07834

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

mQINBGjT6swBEADQkYqo1ohd1NsmQXdS9X2ko8pkzk4mppZdiuWfrN6XUBx5iHa
z
v+CwHoh4NaWs+MDAaB/pYU4ItbcL49pNS1vbUa5lt6b59+OGLGyfQcdoUVM1ur8p
fDEphVDztz58eXrO8ufblGr57m7P3r/uU7kv9oYaVKGpzfpazUh4SYmeehNwNDd2
3vW9J3xchkovInJ7KliGsStrJJ9KUvF16eT8wYsh6Tfr2QMkEhBEMlAjS9CxFtEL
TFNuVtwnFRTmOl3eMa+Gq35QUvFyzu3bouhi4UO3aeZD0Zt0f38tyVUoGrwPYnDZ
/+c+DJ1r4X0Ar/iQA1MLYkoSSChkjSWt/Dvl6O00mvJTmC5jPcrTAAyQBagGyV/w
JvjCctM8RaAWFS/7wkWxf5KvuvPd3kjp8oioENxsi1qwChdgdVliJoMCx9xnSjKq
rX1f9FjlEgCT5njT2XFnfmZifhDA2G3ivVxk0HAEFN5eCPZs7bnV2TFHU91XSVq6
cWgMnP/xpYFR+hApLsPEipHTFcGDJr/O44bDawr2zNWC2mH1Sh73CvOOqzstaftY
DkvmRuUTGJi44JAy1qHXGCePN5DuwW7BEIfq8Kb2HdxqgActbJ6+T/6Q0NyjweHa
wEHBpW8EPbqRe1sCJUswxxwgP1WjaY7Sr1gJyZdEHb5CoJ0D0UFM5ZvAjwARA
QAB
tB9CUEpQSC1DU0lSVCA8Y3NpcnRAaGFsYWwuZ28uaWQ+iQJXBBMBCABBFiE
EEfgb
9TNUQxrwiziX4IgX0eyUddoFAmjT6swCGw8FCQPB9wQFCwkIBwICIgIGFQoJCAs
C
BBYCAwECHgcCF4AACgkQ4IgX0eyUddoUlQ//XyNz9mDJiRNgS/DutDpTX9QxHM6
z
XyesV0+IVwgffkN5uCKDWsqd4LhVuQSNksfZ+ylwaKaatM8k0je6UpcENHEDiN8g
NXRz12x7gvR3t+vYPubiMOBrHjo0fs0SDwAtVpRxWghJZAXYzqYM0mEZR2LJNkU
O
Dfx4Hr6vdn7cfwuc1s9hFmqN9ZRu+S1RhSHAi/H0HoTmZj01qqOs0DpO8Sqb8xF4
H5BYSRCp17ea4SKP3XsIXAGPYBUinhtgZywk0FOSjPvcbC4h2FHoU+TGuibpHvft
03VszVkq7AVAmve/JQzyWg12fFVFADIEhaRQA4f8JyhFHDyeSccyIIriR1vOB19Y
3Q9D9orRKjktEDaR83u0LBYduvxM6Wm1+NBUrxyu71RK/InebzEPwAxHU/O08Hzt
MgiEoNzsyNwVFiTIjHcJ4S1TiAwTOQOML/aP6ultuJxS21CLRKvbh53sir58xpiQ
zpaqhv2A8fIyMZ4JqK8yBEr/K8zY69f4b1a/Qq67Dxq/PljRsFxpzXn2IylgOm7j

q2DBTtcAUhv3kdIUgrRigyjah2PnZ9JorVLkHV+h1DiRgvOxJlS5reLbd6CTP7ik
9v1V8OuYmaL9HqaHBNonT3+KvcmixcLWE+vMO1eyaB+Ryo0cnSrWaLTA5Lb0Mj6
K
pUoLZKiltxeD7Jg=
=nX4a
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://bpjph.halal.go.id/bpjph-csirt/

2.9. Anggota Tim

Ketua BPJPH-CSIRT adalah Kepala Pusat Data dan Informasi BPJPH. Anggota dari BPJPH-CSIRT adalah personel pada Pusat Data dan Informasi, Biro Hukum, Sumber Daya Manusia, dan Hubungan Masyarakat, dan Pusat Pengembangan SDM.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak BPJPH-CSIRT

Metode yang disarankan untuk menghubungi BPJPH-CSIRT adalah melalui *e-mail* pada alamat csirt[at]halal[dot]go[dot]id atau melalui *call center* BPJPH ke 176 pada hari kerja jam 07.30 - 16.00 WIB.

3. Mengenai BPJPH-CSIRT

3.1. Visi

Visi BPJPH-CSIRT adalah terwujudnya tata kelola keamanan dan ketahanan siber di lingkungan Badan Penyelenggara Jaminan Produk Halal yang aman, akuntabel, andal dan profesional.

3.2. Misi

Misi dari BPJPH-CSIRT, yaitu :

a. Melindungi kerahasiaan, integritas, dan ketersediaan informasi serta infrastruktur teknologi yang dikelola;
b. Meningkatkan kesadaran serta kapasitas pemangku kepentingan dalam menjaga keamanan informasi;
c. Memberikan layanan respons insiden yang profesional, akurat, dan dapat diandalkan;
d. Memperkuat kerja sama internal dan eksternal dalam rangka membangun ekosistem keamanan siber yang berkesinambungan;
e. Mendukung terciptanya tata kelola teknologi informasi yang aman, berkelanjutan, dan sesuai regulasi.

3.3. Konstituen

Konstituen BPJPH-CSIRT meliputi Pengguna Teknologi Informasi dan Komunikasi (TIK) sistem elektronik milik Badan Penyelenggara Jaminan Produk Halal.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan BPJPH-CSIRT bersumber dari APBN Badan Penyelenggara Jaminan Produk Halal

3.5. Otoritas

Tim yang bertugas memberikan layanan tanggap insiden siber berupa penanggulangan, pemulihan insiden siber dan layanan manajemen kualitas keamanan di lingkungan Badan Penyelenggara Jaminan Produk Halal

4. Kebijakan – Kebijakan

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

BPJPH-CSIRT melayani penanganan insiden siber dengan jenis berikut :

a. *Web Defacement.*
b. DDoS/DoS.
c. Malware.
d. Phishing.
e. Ransomware.
f. Data breach
g. Pencurian data.
h. Insiden lain yang mengganggu layanan sistem elektronik.

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa BPJPH-CSIRT dapat menggunakan email tanpa enkripsi data (e-mail konvensional) dan call center. Namun, untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi PGP pada e-mail.

5. Layanan

5.1. Penanggulangan dan Pemulihan Insiden Siber

5.1.1. Deteksi Insiden

Layanan deteksi insiden dalam BPJPH-CSIRT mencakup pemantauan berkelanjutan terhadap sistem dan jaringan untuk mengidentifikasi aktivitas mencurigakan, analisis ancaman untuk memahami potensi risiko, serta implementasi sistem peringatan dini yang memberikan notifikasi saat insiden terdeteksi. Tim CSIRT bertanggung jawab untuk merespons insiden dengan prosedur yang jelas, memberikan rekomendasi teknis untuk meningkatkan keamanan, dan menyusun laporan mendetail mengenai insiden yang terjadi. Dengan demikian, layanan ini berperan penting dalam mempercepat respons terhadap insiden, meningkatkan kesadaran keamanan, dan mengurangi risiko terhadap organisasi.

5.1.2. Analisis Insiden

Layanan analisis insiden dalam BPJPH-CSIRT berfokus pada penyelidikan mendalam terhadap insiden keamanan yang terjadi, termasuk pengumpulan dan analisis data untuk memahami penyebab, dampak, dan metode serangan yang digunakan. Tim BPJPH-CSIRT melakukan forensik digital untuk mengidentifikasi jejak penyerang, mengevaluasi kerentanan yang dieksploitasi, dan menilai kerusakan yang ditimbulkan. Selain itu, layanan ini mencakup penyusunan laporan analisis yang mendetail, yang berisi rekomendasi untuk mitigasi dan pencegahan insiden serupa di masa depan. Dengan layanan analisis insiden yang efektif, organisasi dapat meningkatkan pemahaman mereka tentang ancaman yang dihadapi dan memperkuat strategi keamanan siber mereka secara keseluruhan.

5.1.3. Penilaian Risiko Keamanan Siber dan Mitigasi Insiden Siber

Layanan penilaian risiko keamanan siber dalam BPJPH-CSIRT bertujuan untuk mengidentifikasi, menganalisis, dan mengevaluasi potensi risiko yang dapat mengancam aset informasi organisasi. Proses ini mencakup penilaian kerentanan (vulnerability assessment) untuk mengidentifikasi kelemahan dalam sistem dan jaringan, serta pengujian penetrasi (penetration testing) yang mensimulasikan serangan nyata untuk menguji ketahanan sistem terhadap ancaman. Setelah penilaian dilakukan, tim BPJPH-CSIRT menyusun rekomendasi mitigasi yang spesifik untuk mengurangi risiko yang teridentifikasi, termasuk langkah-langkah teknis dan kebijakan keamanan yang perlu diterapkan. Dengan layanan ini, organisasi dapat memahami profil risiko mereka secara menyeluruh dan mengambil tindakan proaktif untuk melindungi aset informasi serta meminimalkan dampak dari insiden siber yang mungkin terjadi.

5.1.4. Pemulihan Insiden Siber

Layanan pemulihan insiden siber dalam BPJPH-CSIRT berfokus pada proses pemulihan sistem dan layanan yang terpengaruh setelah terjadinya insiden keamanan. Tim BPJPH-CSIRT bertanggung jawab untuk mengembangkan dan menerapkan rencana pemulihan yang mencakup langkah-langkah untuk mengembalikan data, memperbaiki kerusakan, dan memastikan bahwa sistem berfungsi kembali dengan aman. Proses ini melibatkan analisis dampak insiden, identifikasi sumber masalah, serta penerapan tindakan perbaikan yang diperlukan untuk mencegah terulangnya insiden serupa. Selain itu, layanan ini juga mencakup komunikasi dengan pemangku kepentingan dan penyusunan laporan pemulihan yang mendetail untuk

evaluasi dan pembelajaran di masa depan. Dengan layanan pemulihan yang efektif, organisasi dapat meminimalkan waktu henti, mengurangi kerugian, dan memperkuat ketahanan mereka terhadap ancaman siber di masa mendatang.

5.1.5. Rekomendasi Pencegahan

Layanan rekomendasi pencegahan dalam BPJPH-CSIRT bertujuan untuk memberikan saran dan strategi yang efektif untuk mengurangi risiko insiden keamanan siber di masa depan. Tim BPJPH-CSIRT menganalisis data dari insiden yang telah terjadi, serta hasil penilaian risiko dan analisis kerentanan, untuk mengidentifikasi langkah-langkah pencegahan yang tepat. Rekomendasi ini mencakup penerapan kebijakan keamanan yang lebih ketat, peningkatan kontrol akses, pelatihan kesadaran keamanan bagi karyawan, serta penerapan teknologi keamanan terbaru, seperti firewall, sistem deteksi intrusi, dan perangkat lunak antivirus. Selain itu, layanan ini juga mencakup pengembangan rencana respons insiden yang komprehensif untuk memastikan bahwa organisasi siap menghadapi potensi ancaman. Dengan layanan rekomendasi pencegahan yang proaktif, organisasi dapat memperkuat postur keamanan mereka, mengurangi kemungkinan terjadinya insiden, dan menciptakan lingkungan yang lebih aman bagi aset informasi mereka.

5.2. Penyampaian Informasi Insiden Siber Kepada Pihak Terkait

Layanan koordinasi insiden kepada pihak terkait dalam BPJPH-CSIRT berfokus pada pengelolaan komunikasi dan kolaborasi yang efektif antara berbagai pemangku kepentingan selama dan setelah terjadinya insiden keamanan siber. Tim CSIRT bertanggung jawab untuk menginformasikan dan berkoordinasi dengan pihak-pihak yang terlibat, termasuk manajemen, tim IT, penyedia layanan eksternal, lembaga penegak hukum, dan Gov-CSIRT, untuk memastikan respons yang terkoordinasi dan efisien. Layanan ini mencakup penyusunan rencana komunikasi yang jelas, penyampaian pembaruan situasi secara berkala, serta pengumpulan umpan balik dari pihak terkait untuk meningkatkan respons. Selain itu, BPJPH-CSIRT juga berperan dalam mengedukasi pemangku kepentingan tentang langkah-langkah yang diambil dan tindakan pencegahan yang perlu dilakukan di masa depan. Dengan melibatkan BPJPH-CSIRT, organisasi dapat memastikan bahwa langkah-langkah yang diambil sesuai dengan kebijakan dan prosedur yang berlaku di tingkat nasional. Dengan layanan koordinasi insiden yang efektif, organisasi dapat memastikan bahwa semua pihak terlibat memiliki pemahaman yang sama tentang

situasi yang dihadapi, mempercepat proses pemulihan, dan meminimalkan dampak dari insiden yang terjadi.

5.3. Diseminasi Informasi untuk Mencegah dan / atau Mengurangi Dampak dari Insiden Siber

Layanan diseminasi informasi dalam BPJPH-CSIRT bertujuan untuk menyebarluaskan pengetahuan dan informasi yang relevan kepada pemangku kepentingan untuk mencegah dan mengurangi dampak dari insiden keamanan siber. Tim CSIRT bertanggung jawab untuk mengumpulkan, menganalisis, dan menyajikan informasi terkini mengenai ancaman, kerentanan, dan praktik terbaik dalam keamanan siber. Layanan ini mencakup penyusunan buletin keamanan, laporan analisis ancaman, dan panduan mitigasi yang dapat diakses oleh seluruh anggota organisasi serta pihak terkait lainnya. Selain itu, BPJPH-CSIRT juga mengadakan sesi pelatihan dan workshop untuk meningkatkan kesadaran dan pemahaman tentang keamanan siber di kalangan karyawan. Dengan diseminasi informasi yang efektif, organisasi dapat memastikan bahwa semua pihak memiliki pengetahuan yang diperlukan untuk mengenali potensi ancaman, mengambil tindakan pencegahan yang tepat, dan merespons insiden dengan cepat, sehingga meminimalkan dampak yang mungkin terjadi.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt[at]halal[dot]go[dot]id dengan melampirkan sekurang-kurangnya :

a. Informasi Kontak Pelapor
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan
c. Kronologi Insiden Siber
d. Dampak serangan

7. *Disclaimer*

BPJPH-CSIRT memberikan respon terhadap pelaporan insiden 1x24 jam. Namun, terkait waktu penyelesaian insiden siber bervariasi sesuai dengan kondisi situasional insiden yang dihadapi.

Plt. Kepala Pusat Data
dan Informasi

Muhammad Djamaluddin