RFC 2350
Tim Tanggap Insiden Siber
Kementerian Perumahan dan Kawasan Permukiman (PKP-CSIRT)

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.1 yang diterbitkan pada tanggal 09 Juli 2025.

1.2. Daftar Distribusi untuk Pemberitahuan

Unit Organisasi, Unit Kerja dan Unit Pelaksana Teknis di lingkungan Kementerian Perumahan dan Kawasan Permukiman.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
http://csirt.pkp.go.id/

1.4. Keaslian Dokumen

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

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 PKP-CSIRT;
Versi	: 1.1;
Tanggal Publikasi	: 09 Juli 2025;
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Tim Tanggap Insiden Siber Kementerian Perumahan dan Kawasan Permukiman
Disingkat : PKP-CSIRT

2.2. Alamat

Pusat Data dan Informasi,
Sekretariat Jenderal, Kementerian Perumahan dan Kawasan Permukiman
Jl. Wijaya I No. 57-59, RT 9/RW 5, Petogogan, Kecamatan Kebayoran Baru, Kota Jakarta Selatan, Jakarta, 12170

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon
Tidak ada

2.5. Nomor Fax
Tidak ada

2.6. Telekomunikasi Lain
Tidak ada

2.7. Alamat Surat Elektronik (*E-mail*)
kemenpkp-csirt@pkp.go.id

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

Bits : 4,096-bit RSA
ID : 062A 7F16 8F9D F134
Key Fingerprint : E6D13098DEEAAC2DCDE4F79F062A7F168F9DF134

Blok PGP Public Key :

-----BEGIN PGP PUBLIC KEY BLOCK-----
mQINBGgO/HEBEACeaTwy27r35zLFDcMx8dntIA6bxEuTXOKCet6Pwc7OJTkig7EG
ZIuejKnEwKIUCe0Nf2Wp2DUTtdMgKWO2BtoiW/Dq9H50x4HpkIGEdYPKNeUbgiVT
U8oaTEz5WGiaBHkDS61D2s1C1dONI3mcqZpwdrxKWAYX3cxeE8o5XxutGWkua3uo
TIUXuZXaAma9yO/6cpaNUvpvliCHmLenDAC+6xO3ZckwNHaMDei9RsXsRbqdDvkX
LFXsArQl/Nn2MNj6AJZeTneD/UvPfWvO80f7Zx5e0oFj7DEmZMgq7PLiODDKS8wY
Shov6Jk8D0X3prORLjNNOIJL3D5ov1yRMjdRvnbFwzIkb+JrnLcN3jRfVdUphFtt
RVzlPBAPqXM6N+hNymLCnYEi5hrEMPeC2SfmYCeWZii357WqlkXKXyns2t0e+rJh
G8h1YWMQ2RAGdcmyuUtV04YreTRnBqp7D6z/RSRG+ddIP4VNRF/TvNKyUb9KLvL
1
lzXY3PBgKMR8Vs4b9uk6ytq4UPaAyDmJwromrdcQ5vVlpnDrd9ju2cMy0BSMvgif
NfzWiUvQjRF6aye1KVLaZUI5aoiWKDj+gc0oTK7epv8A8D89KN3kjTMUWmovQWFN
HtR5Ph8cplsIKGcRm9zz+fu6mBSo5PjSDJVANt70jUAcUq2+PxkR6i3PSQARAQAB
tDBDU0lSVCBLZW1lbnRlcmlhbiBQS1AgPGtlbWVucGtwLWNzaXJ0QHBrcC5nby5p
ZD6JAlcEEwEIAEEWIQTm0TCY3uqsLc3k958GKn8Wj53xNAUCaA78cQIbAwUJBaT6
3wULCQgHAgIiAgYVCgkICwIEFgIDAQIeBwIXgAAKCRAGKn8Wj53xNEk6D/49rdYk
VAkNL3SuyXIUPlVeCMwJEa7z++1T5tEYxpVA7CARNjuGxT6agPdx45sSX1eMEytA
GrG+l2fMf1hGod/kCVMV1KT9pzQ05g8NWVHgFaEDori8dONfozvYoUH6E0/SojTo
LBT84kkCmuN9DIa0Pnx4mTA/+CeSqkgtN7MjGt2ac99uhK3JuxMIlgquNVHAXKJp
sflyL2YyPy4aYZFUppehAg1tv4zPkN/XHg73PGX7bkA+swj+ZiD0UWszlcPzbbma
flvyaHM+1R3IS10LcIa8SSbL78F1bJsLFJFxP05Cz6tH4jUlT8GurY31w4WZo8iR
yu41PJgWYUQvEAdF+0mmavuXgISOyLkWHF+Cdo4s5efrJ7MLlG2c6VKAxdOwzbM+
7LiOR3XfGc4jTaDxdfYlXZapDS9BDlpSAp1w8A7PKQxeVl3QoDcLyFUJ7CjWzD1g
kEvaMMwSeDSrMlOrFNi2r18iVl7njlnkg4iPCihIATbabJABXZwQBBkG2JJrMCZZ
lt+M/9jzvks28AGk3wJmfrDI6eOrv2S/mi1Dpg0bopkWawJULmwXEccjc1HaVE7P
j8/DSYEU53BPAaZC3TfPmlN2VbwC9kUh/QfGfaq2ZENrfpHpd928hrYv88R1eIpe
7k2TzexzMBeUNb8OZKoQYtJMUrerS3NcNq/fArkCDQRoDvxxARAAvPsJ3JA+8IAg
qTqtgPzLHAtoS8/5M+ZB9JigZin8AOmjQlM/06N0H3AWnZyOpR2B/Odf0te21gi9
rBFGXzHqTo8d/uwjrJs0vZPH7sfxmRTj5y+QHJbRSra5m8484K/oIUtj5IKr3kA1
jlv4cMn1zBgGpWJBeHcgXVq/KGSW0XgRV+evalxPm7w0cv1RZczhhhfyDajVMunX
osjHxMCvLsMZb77IuUCJ+IPeWzFJuKKh/pbtHyaARmevR6vEP+siK16VHSJeLSJR

O8w9DPKrMG5rU9sTOfdJPIvK3GBYiCAJevkAvEpY2PWXlGZa3p2ZG7GftA5iv4wB
oXiqaZAbYT4PtzSDV0l+vMFKGb1DKLP2JMCwu0eRocW63Uuk17eW4MlIPbifQ38D
TBPH0wO7Sl9QXD4ubOBO839nestSxVqRcYlpLCtsZ73rvMc3JESq6OrQwLq2Aep7
DQW+lNbA0zTd6byHE/tBhfvhRGDjRCipfqyTlnkwZXceAJk3x0v45+dFa9+lyw4+
fc7NtEEcH88mkbCsiHNS9TD6aDLAkueNkya7ewN322vjskFEuRoZbZ8PV1eBadib
w6MSom9BAD7HHQlYRE+m3+UJ6SK0MwRFtDAxlPe7AaYb7cZwaSljm8Y/9iv6+/vp
SmW+ZYaPDrusTl3jO7TBelplGUDv/PMAEQEAAYkCPAQYAQgAJhYhBObRMJje6qwt
zeT3nwYqfxaPnfE0BQJoDvxxAhsMBQkFpPrfAAoJEAYqfxaPnfE0Ar0P/2ECoGAU
COb9Funfh89dJucdaN+4tHzFE1KGA1V7Ga6j22FFDbpEgoQtr6ZfPnBynLQGD6qj
iXK1PlvBzai0YSXYLdx8c1rfGQDUAzR6X8dwHJ90Ln0uoZWfat3zBfx0nbok+7bz
n6grKMlWvPbEZnbux6AxrhqHlRYF+4W5DoOApwsAQLts2H+WtFavoBydNJSg9BDA
lmRo9WREt7VTtr0kWZGciXskDk/ZNLWvXmLeig4bPgNP14/eIxFYy/6wksDNsAWb
evYq1bkNO4keZzdTrgDgqC0G/9AhFYlFr8m5TGQRsJmPxXTXgZsx7SlpVa3CcQQO
J+XRDuRaGLK/L660J4kRc/QTH2epEj0qwCi6eu4M4g+UGcdXz79FSKiZikEa+4f1
SOefrW0Z1pGl50rhbG7kyIeTn08F0XSK1gg6pJzGXGCcDzkhq8OgJISRcgPpYZZF
qCDa/xEkUyhHpVlRP+ZSe+JQ5uJJiq1YyD3WmCfUt6z6rNhvir3M2jQHXxPPyYFB
dccLKwn3qibMTeo2KDMrRTKALaKTkOXF5QizEH0iIODMXW+2z9VMzxGthteQE0sy
uqyYwxKfhj6neskYgE1fIdtVFxaDi69ZEFnE+FOrTbNg0K2BE0GyYbnf3Sz/v7Da
bLKE/UUuIcIsuaXDgvC7vjYk+CjxSDdgShzf
=eL+I
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
http://csirt.pkp.go.id/

2.9. Anggota Tim

Ketua **PKP-CSIRT** adalah Kepala Pusat Data dan Informasi. Yang termasuk anggota tim adalah seluruh pegawai Pusat Data dan Informasi.

2.10. Informasi/Data lain

Tidak ada

2.11. Catatan-catatan pada Kontak PKP-CSIRT

Metode yang disarankan untuk menghubungi **PKP-CSIRT** adalah melalui *e-mail* pada alamat kemenpkp-csirt@pkp.go.id pada hari kerja jam 07.30 – 16.00 WIB.

3. Mengenai PKP-CSIRT

3.1. Visi

Visi **PKP-CSIRT** adalah pengelolaan sistem keamanan informasi dengan baik dan aman di lingkungan Kementerian Perumahan dan Kawasan Permukiman untuk melindungi aset informasi yang dimiliki oleh Kementerian Perumahan dan Kawasan Permukiman.

3.2. Misi

Misi dari **PKP-CSIRT**, yaitu :

a. Menyediakan layanan keamanan siber teknologi informasi pada Kementerian Perumahan dan Kawasan Permukiman;
b. Meningkatkan kesadaran keamanan siber di lingkungan Kementerian Kementerian Perumahan dan Kawasan Permukiman.

3.3. Konstituen

Konstituen **PKP-CSIRT** meliputi Unit Organisasi, Unit Kerja dan Unit Pelaksana Teknis di lingkungan Kementerian Perumahan dan Kawasan Permukiman.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan **PKP-CSIRT** bersumber dari APBN Kementerian Perumahan dan Kawasan Permukiman.

3.5. Otoritas

Sesuai dengan Keputusan Sekretaris Jenderal Kementerian Perumahan Dan Kawasan Permukiman Republik Indonesia Nomor 158/KPTS/Sj/2025 Tentang Tim Tanggap Insiden Siber Kementerian Perumahan Dan Kawasan Permukiman ditetapkan tanggal 25 Juni 2025

4. Kebijakan – Kebijakan

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

PKP-CSIRT melayani penanganan insiden siber dengan jenis berikut:

a. DDOS;
b. Malware;
c. Ransomware;
d. Phishing;
e. Web defacement;

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

4.3. Komunikasi dan Autentikasi

Media komunikasi untuk informasi dapat menghubungi PKP-CSIRT melalui email kemenpkp-csirt@pkp.go.id.

5. Layanan

5.1. Penanggulangan dan Pemulihan Insiden Siber

5.1.1. Deteksi Insiden

Layanan deteksi insiden dalam PKP-CSIRT mencakup pemantauan berkelanjutan terhadap sistem dan jaringan untuk mengidentifikasi aktivitas mencurigakan dan analisis ancaman untuk memahami potensi risiko. 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 PKP-CSIRT berfokus pada penyelidikan mendalam terhadap insiden keamanan yang terjadi, termasuk pengumpulan dan analisis data untuk memahami penyebab, dampak, dan metode serangan yang

digunakan. PKP-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 PKP-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, PKP-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 PKP-CSIRT berfokus pada proses pemulihan sistem dan layanan yang terpengaruh setelah terjadinya insiden keamanan. PKP-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. Analisis Forensik

Layanan analisis forensik dalam CSIRT bertujuan untuk melakukan penyelidikan mendalam terhadap insiden keamanan siber dengan mengumpulkan, menganalisis, dan menyimpan bukti digital secara sistematis. Tim forensik bertugas untuk mengidentifikasi jejak penyerang, memahami metode serangan, dan menentukan dampak dari insiden tersebut. Proses ini mencakup pengumpulan data dari berbagai sumber, seperti log sistem, perangkat jaringan, dan perangkat penyimpanan, serta penerapan teknik analisis forensik untuk mengungkap informasi yang relevan. Hasil dari analisis ini akan disusun dalam laporan yang mendetail, yang dapat digunakan untuk tindakan hukum, perbaikan kebijakan keamanan, dan peningkatan kesadaran di dalam organisasi. Dengan layanan analisis forensik yang efektif, organisasi dapat memperkuat pertahanan

mereka, memahami pola serangan, dan mengambil langkah-langkah proaktif untuk mencegah insiden di masa depan.

5.1.6. Rekomendasi Pencegahan

Layanan rekomendasi pencegahan dalam CSIRT bertujuan untuk memberikan saran dan strategi yang efektif untuk mengurangi risiko insiden keamanan siber di masa depan. Tim 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 PKP-CSIRT berfokus pada pengelolaan komunikasi dan kolaborasi yang efektif antara berbagai pemangku kepentingan selama dan setelah terjadinya insiden keamanan siber. PKP-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, CSIRT juga berperan dalam mengedukasi pemangku kepentingan tentang langkah-langkah yang diambil dan tindakan pencegahan yang perlu dilakukan di masa depan. Dengan melibatkan Gov-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 PKP-CSIRT bertujuan untuk menyebarluaskan pengetahuan dan informasi yang relevan kepada pemangku kepentingan untuk mencegah dan mengurangi dampak dari insiden keamanan siber. PKP-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, PKP-CSIRT juga mengadakan sesi pelatihan dan sosialisasi 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 kemenpkp-csirt@pkp.go.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*

Penanganan insiden tergantung dari ketersediaan sumber daya dan *tools* yang dimiliki oleh PKP-CSIRT.

Kepala Pusat Data dan Informasi

Adhita Surya Permana, S.Si.,M.T
NIP 197804102002121003