

## RFC 2350 CSIRT JALIN

### 1. Informasi Mengenai Dokumen

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

#### 1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.1 yang diterbitkan pada tanggal 24 Oktober 2024.

#### 1.2. Daftar Distribusi untuk Pemberitahuan

Satuan Kerja di Lingkungan PT Jalin Pembayaran Nusantara (Jalin)

#### 1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada web PT Jalin Pembayaran Nusantara (Jalin)

<https://www.jalin.co.id/id-id/perusahaan/csirt/> (versi Bahasa Indonesia)

#### 1.4. Keaslian Dokumen

Dokumen telah ditanda tangani dengan PGP Key milik CSIRT Jalin. Untuk lebih jelas dapat dilihat pada Sub-bab 2.8.

#### 1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 CSIRT Jalin

Versi : 1.1

Tanggal Publikasi : 24 Oktober 2024;

Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

### 2. Informasi Data/Kontak

#### 2.1. Nama Tim

Computer Security Incident Response Team – PT Jalin Pembayaran Nusantara

Disingkat : **CSIRT Jalin**

#### 2.2. Alamat

Jl. Mega Kuningan Barat Blok Kav.E4.3 No.1-2, RT.5/RW.2, Kuningan Timur, Setiabudi,  
Jakarta Selatan, Jakarta 12950

#### 2.3. Zona Waktu

Jakarta (GMT +07:00)

**2.4. Nomor Telepon**

(021) 1 500 955

**2.5. Nomor Fax**

-

**2.6. Telekomunikasi Lain**

Tidak ada

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

[socteam@jalin.co.id](mailto:socteam@jalin.co.id)

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

**Bit** : 3072

**ID** : 0xEB0027D6CEFAD095

**fingerprint** : 3553 E4D7 EC97 9925 098C 0EC7 EB00 27D6 CEFA D095

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

```
xsDNBGa66XMBDAC+bGp1C5Xsea4ecLAqf8GGWW9pfjxDsmhcCLKPZlwBUx1X6HEU
s1yT6qSelFe6swEbpB38y0xQCBsGnClow/JGUe23wnB2GkOkvu30pTn/Q3nfdeta
kVImx5pKGWWVDYI5HFIGaba4HitkFWvfrSLpMpCcx1zr6fHvs+ma0TIJ+YLTUGYgpmR2IZ
EtJoxZ23vTo7vae1lrGIIBITfPAs0VpM4+97+HX7DrdqRhwoEniFAHXyMn
d9RNEFIXjBdmnfqpPQIWiki6PI1ymR+2gGAQscmasojMcrcHduczJYgmfMzHaG33
/pKizwo9gAI3NHlhy1LuhSORzMkt9BTtoABQFaa5g/SCeYvgydfI5m8JC5AdQ04RN
1hS1VQysJtR7iwUdTS09Q22r+VISplnNa+JsWfXSjnQ3wNpT339IBakTsmvgQNwh
X7GbuPRDj99oe8eA5nh6d899A3wPU6yunjav51IraBmmNxFiUiHDULu2LST2Men8XBwND
qoso/Z0IYUAEQEAAc0fU09DIEphbGluDxTT0N0ZWfTQGphbGluLmNvLmlk
PsLBDQQTAAQgANxYhBDVT5NfsI5kiCYwOx+sAJ9bO+tCVBQJmuulzBQB4TOAAhsD
BAsJCAcFFQgJCgsFFgIDAQAACgkQ6wAn1s760JUATgv9GGAdNv1Nlp6sbUjLjPqA
9xKm6hdMIHRcUxPb1bBIPq05kUtl1wNjx7sreoa8yM1w7N4t8qv0E/I8xeV/bfxk
4iC+enZohKN9YN4E6buR8U7KoJTxF3rcwTEL7KQEAvcxub/d2ZL8W5vUstKpGmr4
3EEpggmZ0/PS9XfR1x7QNdgaxafn3pcwo6bSmCzUV+ThLPc9LiD4W8bj+yoH2PYc
94XGIXbvRuIl756yHaRh53GNUj9mDttWwE8RgTszvXBUqxEWM8S8afuKSHnsaCSZ
56lNyQ0ed6l4ait9mS/iOqFSlp9ompFiEklOidzHXz7IX42EhF5yl+JgFGISfR66
MgnR+wbHOOp5bklSzzaYxeCuenvVxm/UvjFMhc2rcE3OWkMEYkBTgT3NjSDmGyyRg
GMVdlo3ggTBR1gFjeoXKrPFvK9jtVBMVCPTYak85XUb/nkmhPR+vZokYVusv/B/K
HkWiyNtxVYt8eRQ2KrgMtZPG3YRjN/dPhCjUCCjkQ4KJzsDNBGa66XQBDADGEVA+
c16HBAeVrHqs8mUpR6ZJwOeLQHKYM7dJOZBhYehUzYhSDhB3V9cnOzR09PyAKXaJ
r+MA3AODvIzFYhDHe09nba9BDxaAHI8str4gOynUh8/qJsbha16PmgXKTFUkg0ht
zkSYt2mtrkDGdxelkTcyQok7IBaBBPh3Tcb9kZBpzeNlqini1/4zBTui2CZC2WgR
```

ieMf77MYQVXrrP21ALvOHws/eCJS8nJxGTnmrZELjsKLayc/atI6yFfbXVgLmS  
p9ySPbwm6tqLdspMm/xBTS96T8zmuC6iwlH+sPeol4jLvUlybCtNQaRAgMaMpuGHhI2jge+  
yIK6gPOEZMok7/4M+nGUDNdsLQfuSO1akWdcFvHv5ihWKTwaLo8kILkd59MeJ0DN6cbik  
UoMzp31sxeOKdVsBGolSTjDT1h+QL+rJaNA0/IRPsMQ77vcvx7ln  
LPMavfRNWxyUPNA84i5MZI6mylyy36sZvdK4j+zWZBqQO7iwSQxZTwnpgfkAEQEA  
AcLA/AQYAAQgAJhYhBDVT5NfsI5kICYwOx+sAJ9bO+tCVBQJmuul0BQkB4TOAAhsM  
AAoJEosAJ9bO+tCVJNAL/2aBifDxWvUczGEz8ir+K7Kwwj9v64O+kqAdSOGqft50  
6x6fH9OZblw691fMhnhXRNbhW0JN/ILpSYF83PDyO779bSN2is9CkLw1Uh+boAio  
cVfezmWNxTXe64M3h5BwQ6Vdw5O+kZL3WlvfHI8v7hyLriuKWep24bfQEwgOr8lc  
HCaqeFLBUtz37fc/CbU8DZub5LvjdjCw+cxUIUAkKLCYfXI5K0KPhJrwdDT7gC3Xi  
s9YdLgK4aTxp3+bqIjHtAXEvuwX2pQ1i9Gajny/cReS1wgZRTHV5jeJZi+cHVxch  
1pyUilsuN5rcdq+jetytP7lm/iDGOt62kZSX1CX4+LnEO79/p0H7ShK94NXRygyf  
bTWGtcgF7Nft7y2EwWOsSYIIoxc6gFIVOnnpFnHr2YFOXSFusWYI8a/gcF5Np8cNpLbkG8  
Y+KnW/Gc/HcYX2f8ferl1QwR/6CbnDiv/X7D/5FdbM1SCTs+R9t4zHwGn1  
aWzut5zb2QApnufwfdldhw==  
=Oz0j  
-----END PGP PUBLIC KEY BLOCK-----

## 2.9. Anggota Tim

Ketua CSIRT dijabat oleh Pimpinan Departemen (Vice Presiden) IT Security & Continuity Management. Susunan anggota CSIRT Jalin ditetapkan oleh Pimpinan Departemen (Vice Presiden) Human Capital Management. Untuk organisasi CSIRT Jalin merujuk kepada Surat Keputusan Kepala Departemen Human Capital Management Nomor : SK.06.15.03./r.0.0/HCM10000000/JPN/2024 PT Jalin Pembayaran Nusantara Tentang Pembentukan Computer Security Incident Response Team (CSIRT).

## 2.10. Informasi/Data lain

Tidak ada

## 2.11. Catatan-catatan pada Kontak PT Jalin Pembayaran Nusantara

Metode yang disarankan untuk menghubungi PT Jalin Pembayaran Nusantara adalah melalui *e-mail* pada alamat [socteam@jalin.co.id](mailto:socteam@jalin.co.id) atau melalui nomor telepon (021) 1 500 955 yang siaga selama 24/7.

## 3. Mengenai CSIRT Jalin

### 3.1. Visi

Visi CSIRT Jalin adalah terwujudnya ketahanan siber yang andal dan profesional di lingkungan PT Jalin Pembayaran Nusantara.

### **3.2. Misi**

Misi dari CSIRT Jalin, 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 dan serangan yang menimbulkan gangguan, kegagalan dan kerugian
- c. Menyediakan mekanisme penanggulangan insiden dan/atau pemulihan insiden yang dilakukan oleh tim penanggulangan dan pemulihan insiden siber

### **3.3. Konstituen**

Konstituen CSIRT Jalin meliputi:

- a. Pengguna pengguna teknologi informasi di lingkungan PT Jalin Pembayaran Nusantara
- b. Seluruh konstituen anggota CSIRT Jalin melaksanakan rekomendasi dan/atau imbauan yang dikeluarkan oleh CSIRT Coordinator dari CSIRT Jalin.

### **3.4. Sponsorship dan/atau Afiliasi**

CSIRT Jalin merupakan bagian dari PT Jalin Pembayaran Nusantara sehingga seluruh pendanaan untuk penyelenggaraan berasal dari:

- a. Anggaran operasional PT Jalin Pembayaran Nusantara

### **3.5. Otoritas**

Berdasarkan Surat Keputusan Kepala Departemen Human Capital Management Nomor : SK.06.15.03./r.0.0/HCM10000000/JPN/2024 PT Jalin Pembayaran Nusantara Tentang Pembentukan Computer Security Incident Response Team (CSIRT), PT Jalin Pembayaran Nusantara berwenang untuk melakukan pengelolaan insiden keamanan TI secara proaktif dan reaktif.

## **4. Kebijakan – Kebijakan**

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

Dukungan yang diberikan oleh CSIRT Jalin kepada konstituen dapat bervariasi tergantung dari jenis dan dampak insiden seperti dibawah ini namun tidak terbatas pada:

- a. *Distributed Denial Of Services (DDOS)*
- b. *Malware*
- c. *Phishing*
- d. *Compromised Information*
- e. *Unauthorized Activity*
- f. *Brute Force Attack*
- g. *Email Spam*

#### **4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data**

CSIRT Jalin 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 CSIRT Jalin harus dirahasiakan.

#### **4.3. Komunikasi dan Autentikasi**

Untuk komunikasi biasa CSIRT Jalin 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 Proaktif**

Layanan proaktif dari CSIRT Jalin yaitu :

- 5.1.1. Memberikan update informasi terkait *vulnerability* yang muncul dan juga memberikan masukan untuk meningkatkan standar keamanan
- 5.1.2. *Me-monitor*, melakukan review dan mengkomunikasikan perkembangan standar keamanan termasuk terhadap penggunaan sistem/teknologi baru berdasarkan tren yang terjadi untuk mengidentifikasi ancaman potensial yang mungkin terjadi
- 5.1.3. Mengembangkan penggunaan perangkat *security* untuk meningkatkan standar keamanan yang ada
- 5.1.4. Menyelenggarakan layanan Tim Tanggap Insiden Siber sebagaimana dimaksud dalam diktum Kelima dan hal-hal lain yang dibutuhkan Perusahaan tentang penanganan Insiden Siber di Perusahaan;
- 5.1.5. Mengoordinasikan penanganan Insiden Siber tingkat Perusahaan;
- 5.1.6. Merumuskan panduan teknis penanganan Insiden Siber;
- 5.1.7. Menjadi narahubung Perusahaan dan melakukan tugas koordinasi apabila terjadi insiden siber;
- 5.1.8. Melakukan koordinasi dengan Tim Tanggap Insiden Siber sektoral atau dengan Tim Tanggap Insiden Siber nasional dalam hal belum tersedianya Tim Tanggap Insiden Siber sektoral;
- 5.1.9. Melakukan penanggulangan dan pemulihan insiden secara cepat dan tepat;
- 5.1.10. Memberikan bantuan yang diperlukan kepada pihak yang menerima layanan;
- 5.1.11. Melakukan forensik untuk mengidentifikasi, mengoleksi, menganalisa dan menguji bukti digital atau mengekstrak bukti dari computer atau perangkat seperti perangkat digital atau perangkat IT lainnya dan kemudian digunakan sebagai bukti dalam kasus hukum atau untuk tujuan investigasi;

- 5.1.12. Memberikan laporan penanganan Insiden Siber yang telah terjadi kepada *Board of Directors* dan Tim Tanggap Insiden Siber sektoral atau Tim Tanggap Insiden Siber nasional dalam hal belum tersedianya Tim Tanggap Insiden Siber sektoral; dan
- 5.1.13. Melakukan koordinasi dan/atau kerja sama dengan pihak lain dan seluruh pemangku kepentingan dengan memperhatikan kerahasiaan informasi, perlindungan data, dan sesuai dengan ketentuan peraturan perundangan-undangan.

## **5.2. Layanan Reaktif**

Layanan reaktif dari CSIRT Jalin yaitu :

- 5.2.1. Memberikan alert ataupun *warning* terkait insiden keamanan TI yang terjadi dan tindakan yang diperlukan untuk pengamanan atau perbaikan sistem
- 5.2.2. Pengelolaan dan koordinasi di dalam penanganan insiden keamanan TI yang terdeteksi
- 5.2.3. Melakukan analisa dan pengelolaan terhadap bukti-bukti yang ditemukan

## **6. Pelaporan Insiden**

Laporan insiden keamanan siber dapat dikirimkan ke [socteam@jalin.co.id](mailto:socteam@jalin.co.id) dengan melampirkan sekurang-kurangnya :

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

## **7. Disclaimer**

Tidak ada