

## RFC 2350 DSG - CSIRT

### 1. Informasi Mengenai Dokumen

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

#### 1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 15 Februari 2024.

#### 1.2. Daftar Distribusi untuk Pemberitahuan

Satuan Kerja di lingkungan PT Digital Solusi Grup, dan anak perusahaannya.

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

Dokumen ini tersedia pada:

<https://csirt.dsg.id> (versi Bahasa Indonesia)

#### 1.4. Keaslian Dokumen

Dokumen telah ditanda tangani dengan PGP Key milik **PT Digital Solusi Grup**. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

#### 1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 **DSG - CSIRT**;

Versi : 1.0;

Tanggal Publikasi : 15 Februari 2024;

Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

### 2. Informasi Data/Kontak

#### 2.1. Nama Tim

Digital Solusi Grup – Computer Incident Respond Team  
Disingkat : **DSG – CSIRT**.

#### 2.2. Alamat

Jl. Raya Sawojajar No. 12 Blok NY-01, Sawojajar, Kec. Kedungkandang, Kota Malang, Jawa Timur.

#### 2.3. Zona Waktu

Kota Malang (GMT+07:00)

**2.4. Nomor Telepon**

(0341) - 3024534

**2.5. Nomor Fax**

-

**2.6. Telekomunikasi Lain**

(+62) 812 3334 5119 (WhatsApp)

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

info[at]dsg[dot]id

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

Bits : 4096

ID : 8C2E9F415EC150F7

Key Fingerprint : 116C7D30F09758ADDC971B4F8C2E9F415EC150F7

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

```
mQINBGXNb8IBeadfp1YSKj3hhMTPRZUz8BEVcXQWjOTS6N0jRC2ji9YSelfc3UI
D
SlzAwLjVkmFnbhSV62hjL3wcoo2y5HPb0kS1NF46FvdnQWpo2DBPRos/VlflOwiL
V0YYG3ax7r1tZ6vAa10tcxN3mS/s6bceUUZNYQ+qxolWEOogZjIlyFH+nUsRYyBz
maKhr97SVODk+KbOr24b1rnZowzsOA+78e2UezrTPi3uxkrq0yM1tzPiErWXG462
Pg/OpHIgCcJ6Kv4b0qJ22AMjdUq2MkF3o9Qmse9M0zrReHhUoYsvbLeCJfrotUEb
usNT2VHTTh1htNIMEK0mob/2+ojqjKT9g6BqXubX/iFgljdUvc34E28V1/HrkEuqU
spRhfY4i9A67GCzq17G/ATEDL4Q8cwvBGJj1GLwvplqRAWmQlwljkfMj63JMIg0
O5zDoPAhWI91jEOB6/jNLVu6JGqWtEbv5bAzQrSjdbgNDdlQkjtD6+RMJ7Pn4Cf
fLhju9n2G5hptCPxJR0paA0UWtzHGRph7uTRAg8uZeD49sh+dLmoDQXRRPJzqxl
e
o6KzrSIbAkmKdpJX+8JBFK/ZcbpuQ9xwxAgZ//1upS7IjCvYKp2Mfoev233yqTTI
9QVSCDbWUyE10kmal3O84iMf+7UkgwiBMGChInxKwSf87eijpbHgxb8SNQARAQ
AB
tCRQVCBEaWdpdGFsIFNvbHVzaSBHcnVwIDxpbmZvQGRzZy5pZD6JAK4EEwEK
ADgW
IQQRbH0w8JdYrdyXG0+MLp9BXsFQ9wUCZc1vwglbAwULCQgHAgYVCgkICwIEF
gID
AQIeAQIXgAAKCRCLp9BXsFQ9z7bEADXA68QNCrp0Z5J+TJ/3oUgRsx78XY6F
Yhw
XZphSNmyVrbQ3nmDhRU+a1CnRa/vHWNesC0cyEumRU1fVIClo4CHiN4cERFkn
5sN
IbDFe/SY3QAY5WmEivqXh6i6LY5rqBQgNmvlhBMo2Q3cBAKn/D7GjYWbTI4gONs
y
```

**Head Office**

Ruko WOW Blok N/Y 1,  
Jl. Raya Sawojajar No.12, Sawojajar,  
Kedungkandang, Kota Malang,  
Jawa Timur 65139, Indonesia

**Representative Office**

Gedung Centennial Tower Lv. 29 Unit D-E,  
Jl. Jenderal Gatot Subroto Kav 24-25  
Karet Semanggi Setiabudi Jakarta Selatan,  
DKI Jakarta 12930, Indonesia

**Contact**

🌐 [www.digitalsolusigrup.co.id](http://www.digitalsolusigrup.co.id)  
✉ [info@digitalsolusigrup.co.id](mailto:info@digitalsolusigrup.co.id)  
☎ 021-29608319

O4pMZVG6oIUQW8oNRWYaVEo77sIPP3COTXY3bCA1309YJa9iv7IDURcmR1XD  
eFeg  
qdI4o7hCxeG7bA5yoGnqwyT8BAQwDuMBbc7ptQwjKw3GmUha8ojit3ZZ/36Uf4E+  
E4NnbiUuyhunBnDkx+HigzqxqCddrWE7NdwDD/GtbUIPaVNAkqorZCtROr23HJsRg  
kFcBjYTVI2I9iR7nPw9EGNr+R65prH8pDmB0ZFw7AowaAIYkMa15TCB65UXKrZ8  
7  
zaYrudi9EUABzsw+GqvN3Y8ZD5ksI7c/XrNyHev/e33hKIX5pverez47rYI1Dj1b  
p8PkSwDVBSMZ/nVquHh2LP0msbgvEjg7U6rmsxefsmU9F6TBtSDkrhM/KLni/DI3  
qG9EdzVbr1szqIE4XAc/QQlXuXgSyXynEuKTTn8i9UpjFYxtnbsSyBW7Hq2jSn1/  
ZxBM/YC8e9+oyHesMY3YPTo5O6PbqImJ+ePDby2+29fktzggMyEH8e9N1xmmHX  
U5  
FJxgMPWY9LkCDQRizW/CARAA91INhQ89Q5eEZHN1004E1TKulrBwOKPgCgOgt  
iPZ  
oQ2qcq4IWjyTW0dSTTJS5p+sFFDAoAcanG7qorThIDKpuNlu2O8Wbl5+p5DjvvgV  
5jRWhgsjTGsDX+JIYLi3fD6TmC63DNbOofk8bR/V4JzsigERR9JQGRKdTgcGNe1o  
t/bGwkaKCbKxGyFrhVixk8Nq/yIbJLh9oz7KV/iovEsNSZMs5WJ9r0yJ5GcSR6nk  
OkprERqnbBwELfGA8mXiRhpEy3zbR9vhPU5FibyAoLHWU/CcFPwm0eWQoGKu  
yA4  
aePrBDApCqjqMsX6IX6zM478DxFuK7+aWdagT96ZbzQ97A1Owhu5MypcatO6qH  
Mo  
q9t6qQVVcnCLE4hDwx2u3g/RBr/PhPc/oRbgl24K7GxQ3IVzUVJIRZWQbNLd+p0X  
D9xNTcmWwVi3Du9pXNedZy18wyUBImajHN+csxwHDGRiCzFXt8w3x0kSlEkV4O  
X6  
kaK/OSKsCcxVoZpsesB8F1ua+ijCGHTWOkDG7KkbShqEu+3nSx6RqV/Ga1ctfR5g  
Q  
n+XQQtJmcbXe0NxtgA0Izvxz9t7iMmykq5w6nTnJIHCXbCrl+7y0RIO2byMTgin  
z5ZGRPtgDAVOt1w132cRXP2MDg8WO475yhrPKBnGL5v606++fxHLVLWae06e  
uWS  
IGEAEQEAAYkCNgQYAQoAIBYhBBFsfTDwl1it3JcbT4wun0FewVD3BQJlzW/CAhs  
M  
AAoJEIwun0FewVD3WEIP/0NUgh5mTDTD0SsoVK0xyzd8eIBSTfV6ox8dvtxE7Hs  
B  
UTcCjPX3r0C3JPQeTMx4p+egIVx6jePqShKqQs3hQ9/bd1YhIUBtFJJb7WEcz2s0  
o5nCXS9SfQ7/hOLobkXLVkeZ+rfI0OJwrSizZiuNoT14psBVxplF5spVsX1+rBu+  
O3NLsnAlw6xIH8z6z7CGVsGfl9bLfPRM5r0/BqkxIXvS/Xi7CGBQgQGnN6o7C9uR  
qi0BO6U4XWMgb2IJeHvkHTA1BQmBsaYrzjk/VFT0u/Vt1/lhnBKZzGhcAHwqw0NW  
J+PQAZWodXvSe559IUN/8td0b6e7ohvro+2qbAB3VqAvRuM4aDYK6122+/+Am2b  
3  
o1M7fsJIW4PfZoPyRgf8rkTkMvG2c1NcG3IHvmfK+wjx5VR2ApFpkawLEf8R50EW  
kw8v+DowYiPKPRjSX0oL08QijmWrTvtwfe2BBSWjR0C5ODYclUvgHYn3qaY/nat+  
vdF4ZG9vvl60MGC84mS/MP1VwWHEoZP/nkT5SN39OTi2Nni8AUv8OMbJU4hnW  
z0p  
CtMEkPbMdWfQ2y5pAkrPGd4atxU0iEzfY8YWP+GPAZrYwtXKkWCd2GrDPgEBCc  
BC  
SsGSRAE6hickM/FN7fWINGtOkhYgDZeqazjSqJ2f1/MBnDw4LtlP0tnA2QLJWwBN  
=Mxyp

**Head Office**

Ruko WOW Blok N/Y 1,  
Jl. Raya Sawojajar No.12, Sawojajar,  
Kedungkandang, Kota Malang,  
Jawa Timur 65139, Indonesia

**Representative Office**

Gedung Centennial Tower Lv. 29 Unit D-E,  
Jl. Jenderal Gatot Subroto Kav 24-25  
Karet Semanggi Setiabudi Jakarta Selatan,  
DKI Jakarta 12930, Indonesia

**Contact**

[www.digitalsolusigrup.co.id](http://www.digitalsolusigrup.co.id)  
[info@digitalsolusigrup.co.id](mailto:info@digitalsolusigrup.co.id)  
021-29608319

-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada:

[https://csirt.dsg.id/assets/CSIRT-DSG\\_8C2E9F415EC150F7\\_public.asc](https://csirt.dsg.id/assets/CSIRT-DSG_8C2E9F415EC150F7_public.asc)

## 2.9. Anggota Tim

Ketua **DSG - CSIRT** adalah Dean Diyantha Putrandi. Yang termasuk anggota tim adalah seluruh anggota tim Security Engineer PT Digital Solusi Grup.

## 2.10. Informasi/Data lain

Tidak ada.

## 2.11. Catatan-catatan pada Kontak **DSG – CSIRT**.

Metode yang disarankan untuk menghubungi **DSG – CSIRT** adalah melalui *e-mail* pada alamat `csirt[at]dsg[dot]id` yang siaga selama 24/7.

## 3. Mengenai **DSG – CSIRT**

### 3.1. Visi

Visi **DSG – CSIRT** adalah Menjadi pemimpin di industri keamanan informasi dengan memberikan respons yang cepat, tangkas, dan efektif terhadap insiden keamanan, serta menjadi mitra terpercaya dalam melindungi aset digital klien kami dari ancaman cyber

### 3.2. Misi

Misi dari **DSG – CSIRT**, yaitu :

- a. Memberikan respons yang cepat dan efektif terhadap insiden keamanan yang melibatkan sistem dan jaringan klien kami, dengan focus pada mitigasi risiko dan pemulihan yang cepat.
- b. Mengidentifikasi, menganalisis, dan mengatasi ancaman cyber dengan menggunakan teknologi canggih dan metodologi baru, serta berkolaborasi dengan Lembaga keamanan lainnya.
- c. Membangun kesadaran keamanan yang kuat di seluruh organisasi klien kami melalui penyuluhan, pelatihan, dan penyediaan sumber daya yang relevan.
- d. Mengembangkan dan mengimplementasikan kebijakan, prosedur, dan praktik terbaik dalam perlindungan siber untuk membantu klien kami mengurangi risiko keamanan secara proaktif.
- e. Berkomitmen untuk terus meningkatkan kemampuan teknis dan pengetahuan anggota tim CSIRT melalui pelatihan reguler dan pengembangan profesional.
- f. Berperan aktif dalam komunitas keamanan informasi dengan berbagi pengetahuan berpartisipasi dalam forum industry, dan berkontribusi pada upaya kolaboratif dalam menghadapi ancaman siber.

### 3.3. Konstituen

- a. Konstituen **DSG – CSIRT** adalah seluruh divisi dalam PT Digital Solusi Grup, dan anak perusahaannya.

### 3.4. Sponsorship dan/atau Afiliasi

-

### 3.5. Otoritas

Otoritas dari **DSG – CSIRT** memberikan layanan tanggap insiden siber berupa layanan reaktif, layanan proaktif, dan layanan manajemen kualitas keamanan di lingkungan PT Digital Solusi Grup.

## 4. Kebijakan – Kebijakan

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

**DSG – CSIRT** melayani penanganan insiden siber dengan jenis berikut :

- a. Malware Detection,
- b. Web Threat Protection
- c. Exploit Defense
- d. Network Attack Defense (NAD)
- e. Fileless Attack Defense
- f. Ransomware Mitigation and Recovery
- g. Attack Forensics, and Visualitation

Dukungan yang diberikan oleh **DSG – CSIRT** pada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden.

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

- a. Kerja sama antar perusahaan dapat dilaksanakan dengan tujuan untuk saling berbagi sumber daya pengetahuan, keterampilan dan informasi mengenai keamanan siber dan serangan siber agar dapat melakukan mitigasi atas potensi serangan serupa atau turunannya.
- b. Kerjasama antar perusahaan mitra PT Digital Solusi Grup dilakukan dengan tetap memperhatikan kebijakan, sistem prosedur, dan perlindungan kepentingan masing-masing pihak yang terlibat.

### 4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa dengan **DSG – CSIRT** dapat menggunakan alamat *e-mail* tanpa enkripsi data (*e-mail* konvensional). Namun, untuk komunikasi yang memuat informasi sensitive/terbatas/rahasia dapat menggunakan enkripsi PGP pada *e-mail*.

## 5. Layanan

### 5.1. Layanan Utama

Layanan utama dari **DSG – CSIRT** yaitu :

#### 5.1.1. Pemberian Peringatan Terkait Keamanan Siber

#### Head Office

Ruko WOW Blok N/Y 1,  
Jl. Raya Sawojajar No.12, Sawojajar,  
Kedungkandang, Kota Malang,  
Jawa Timur 65139, Indonesia

#### Representative Office

Gedung Centennial Tower Lv. 29 Unit D-E,  
Jl. Jenderal Gatot Subroto Kav 24-25  
Karet Semanggi Setiabudi Jakarta Selatan,  
DKI Jakarta 12930, Indonesia

#### Contact

🌐 [www.digitalsolusigrup.co.id](http://www.digitalsolusigrup.co.id)  
✉ [info@digitalsolusigrup.co.id](mailto:info@digitalsolusigrup.co.id)  
☎ 021-29608319

Pemberian peringatan dilakukan secara real-time dengan mengamati sistem dan memberikan laporan anomali maupun insiden yang terjadi melalui email yang dipantau oleh tim CSIRT dan di informasikan kepada pihak terkait di dalam Perusahaan.

### 5.1.2. Penanganan Insiden Siber

Penanganan Insiden Siber dilakukan oleh tim **DSG – CSIRT** melalui beberapa tahapan diantaranya:

1. **Deteksi Insiden:** **DSG – CSIRT** menggunakan berbagai alat dan teknologi untuk mendeteksi indikasi insiden keamanan, seperti sistem deteksi intrusi (IDS), sistem deteksi ancaman (TDS), dan pemantauan aktivitas jaringan. Selain itu kami juga mengandalkan laporan manual dari pengguna atau sistem otomatis pemicu alarm.
2. **Evaluasi dan Klasifikasi:** Setelah mendeteksi insiden, kami melakukan evaluasi awal untuk menentukan tingkat keparahan dan dampak insiden terhadap operasi bisnis dan data klien. Insiden kemudian diklasifikasikan berdasarkan tingkat kepentingan dan prioritas penanganan.
3. **Respon Cepat:** Tim CSIRT kami memberikan respons cepat terhadap insiden dengan mengisolasi sumber insiden, menonaktifkan akses yang tidak sah, dan menghentikan penyebaran lebih lanjut dari serangan tersebut. Tindakan ini dilakukan untuk meminimalkan dampak insiden dan mencegah kerusakan yang lebih besar.
4. **Investigasi Mendalam:** Setelah mengambil tindakan respons awal, tim kami melakukan investigasi menyeluruh untuk memahami sumber, metode, dan dampak insiden dengan lebih detail. Ini melibatkan pemantauan aktivitas jaringan, dan penelusuran jejak digital untuk mengidentifikasi pelaku dan motif serangan.
5. **Pemulihan:** Kami melakukan pemulihan sistem dan data yang terpengaruh oleh insiden dengan mengembalikan keadaan keamanan yang stabil dan memastikan integritas data kembali normal. Ini melibatkan pemulihan dari cadangan data, perbaikan kerentanan keamanan, dan penerapan langkah-langkah perlindungan tambahan untuk mencegah insiden serupa di masa depan.
6. **Pelaporan dan Komunikasi:** Kami memberikan laporan insiden yang terperinci kepada manajemen perusahaan, klien yang terkena dampak, dan otoritas terkait sesuai dengan regulasi dan kebijakan yang berlaku. Komunikasi terbuka dan jujur sangat penting dalam memastikan transparansi dan membangun kepercayaan dengan semua pihak terkait.
7. **Evaluasi Pasca-insiden:** Setelah insiden diselesaikan, kami melakukan evaluasi pasca-insiden untuk mengevaluasi efektivitas respons kami, mengidentifikasi pembelajaran dan peluang perbaikan, serta merekomendasikan tindakan pencegahan lebih lanjut untuk meningkatkan ketahanan keamanan di masa depan.

## 5.2. Layanan Tambahan

Layanan tambahan dari **DSG – CSIRT** yaitu :

#### **5.2.1. Penanganan Kerawanan Sistem Elektronik**

Layanan ini kami berikan dalam lingkup kerja PT Digital Solusi Grup sebagai layanan penuh dalam perilaku *pre-execution* maupun *post-execution* secara utuh.

#### **5.2.2. Pemberitahuan Hasil Pengamatan Potensi Ancaman**

Pemberitahuan hasil pengamatan potensi ancaman diberikan dalam bentuk laporan mingguan dan bulanan, serta terdapat laporan untuk kegiatan pengamatan yang diperlukan tindakan penanganan segera.

#### **5.2.3. Pendeteksian Serangan**

Pendeteksian serangan dilakukan dengan teknologi otomatis dan manual dalam lingkup infrastruktur maupun jaringan, endpoint, dan cloud server.

#### **5.2.4. Analisis Risiko Keamanan Siber**

Layanan ini diberikan dalam bentuk sajian data visualisasi terkait jaringan yang terjangkit malware atau berpotensi terjangkit malware maupun ransomware.

#### **5.2.5. Konsultasi Terkait Kesiapan Penanganan Insiden Siber**

Layanan ini diberikan oleh Lead Auditor dan Lead Implementor bersertifikasi dari BSI dengan standar ISO 27001:2022.

#### **5.2.6. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber**

Tim CSIRT bertanggung jawab memberikan layanan Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber secara rutin dari hasil temuan nyata yang diperoleh dalam perusahaan, juga informasi yang dibagikan oleh tim CSIRT eksternal.

## **6. Pelaporan Insiden**

Laporan insiden keamanan siber dapat dikirimkan ke [csirt\[at\]dsg\[dot\]id](mailto:csirt[at]dsg[dot]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**

Informasi yang disediakan di atas dimaksudkan untuk tujuan penyuluhan dan informasi umum saja. Meskipun upaya telah dilakukan untuk menyajikan informasi yang akurat dan terpercaya, perlu diingat bahwa tidak ada tindakan atau langkah keamanan yang dapat menjamin perlindungan yang sepenuhnya efektif terhadap serangan siber. Setiap organisasi atau individu harus mempertimbangkan risiko unik dan mengambil langkah-

langkah keamanan yang sesuai dengan situasi mereka. Selain itu, tidak ada sistem atau jaringan yang kebal terhadap serangan siber, dan serangan dapat terjadi meskipun telah diimplementasikan tindakan pencegahan yang kuat. Oleh karena itu, penting untuk terus memantau, memperbarui, dan meningkatkan keamanan informasi secara berkala sesuai dengan perkembangan teknologi dan ancaman siber yang terus berubah. Tindakan proaktif dan responsif adalah kunci untuk mengurangi risiko dan memitigasi dampak serangan siber.

Hormat kami,

**Dean Diyantha Putrandi**  
**Direktur Utama**

**Head Office**

Ruko WOW Blok N/Y 1,  
Jl. Raya Sawojajar No.12, Sawojajar,  
Kedungkandang, Kota Malang,  
Jawa Timur 65139, Indonesia

**Representative Office**

Gedung Centennial Tower Lv. 29 Unit D-E,  
Jl. Jenderal Gatot Subroto Kav 24-25  
Karet Semanggi Setiabudi Jakarta Selatan,  
DKI Jakarta 12930, Indonesia

**Contact**

[www.digitalsolusigrp.com](http://www.digitalsolusigrp.com)  
[info@digitalsolusigrp.com](mailto:info@digitalsolusigrp.com)  
021-29608319

