Government Technology Agency
GITSIR RFC 2350 Profile

Version 1.0

Government IT Security Incident Response Team

01 March 2023

1. GITSIR RFC 2350 Profile

The GITSIR RFC 2350 profile contains information about GITSIR Team. RFC 2350 is commonly adopted as the framework for CERTs/CSIRTs to disseminate information on which constituency and services are covered.

1.1. Abbreviation

ACISO/SIRO	Agency Chief Information Security Officer/Security Incident Response Officer
CERTs	Computer Emergency Response Teams
CSIRTs	Computer Security Incident Response Teams
FIRST	Forum of Incident Response and Security Teams
GIROC	Government Incident Reporting & Operation Centre
GITSIR	Government IT Security Incident Response
GovTech	Government Technology Agency
ICT&SS	Infocomm Technology & Smart Systems
ISPs	Internet Service Providers
RFC	Request For Comments
SE3	Secure Email 3
SNDG	Smart Nation Digital Government

2. Document Information

This document describes the Government IT Security Incident Response (GITSIR) team in accordance with RFC 2350. It provides information about which constituency GITSIR serves and the services offered by GITSIR.

2.1. Date of Last Update

01 March 2023

2.2. Locations where this document may be found

GITSIR RFC 2350 Profile is published on GovTech Corporate Website.

3. Contact Information

3.1. Name of the Team

GITSIR (Registered name with FIRST: SG-GITSIR)

3.2. Address

Government Technology Agency of Singapore
10 Pasir Panjang Road
#10-01 Mapletree Business City
Singapore 117438

3.3. Date of Establishment

1997

3.4. Time zone

Singapore (GMT +0800)

3.5. Telephone number

Incident Reporting Hotline: +65 6211 0070 / +65 9223 9887

3.6. Other Telecommunication

Not Applicable

3.7. Electronic Mail Address

GITSIR@tech.gov.sg

3.8. Encryption Information

Secure Email 3 (SE3) should be used as far as possible when encrypted communication is required.

3.9. Team Members

The Head of GITSIR is Mathew Soon (mathew_soon@tech.gov.sg). The team consists of cybersecurity engineers from Government Technology Agency (GovTech).

3.10. Points of Contact

GITSIR provides a 24/7 standby incident response service.

Regular response hours: Monday - Friday, 0800H to 2000H (excluding Public Holidays)

4. Charter

4.1. Mission Statement

The mission of GITSIR is to defend public sector systems against cyber and data threats through decisive operational detection and response capabilities as a harmonious, open and trusting (HOT) team.

4.2. Constituency

GITSIR is the Cyber Security Incident Response (CSIRT) team for Infocomm Technology & Smart Systems (ICT&SS) within the Singapore public sector, which includes all Government Ministries, Organs of State, Departments, and Statutory Boards. It is responsible for supporting cybersecurity detection, incident response and investigations, as well as providing cybersecurity resources such as directives, advisories, instructions and playbooks on cybersecurity vulnerabilities and threats.

4.3 Sponsorship and/or Affiliation

GITSIR is part of GovTech, which is a Singapore Government agency, GovTech is the implementing arm of the SNDG Office, which drives the digital transformation of Government. GovTech is also the sector lead for cybersecurity in the Singapore Government, responsible for the safety and security of Government digital structures.

GITSIR is affiliated with FIRST, the global Forum of Incident Response and Security Team.

4.4. Authority

As a Government agency, the tasks and mandate of GITSIR and its parent organisation GovTech are stated under the GovTech Act 2016.

5. Policies

5.1. Types of Incidents and Levels of Support

GITSIR provides 24/7 (standby) cybersecurity incident response support to deal with the Government's central infrastructure services providers, local law enforcement or other entities.

GITSIR develops and maintain the Whole of Government (WoG) Cybersecurity Incident Management (IM) Standing Operating Procedure (SOP), which defines the policies, processes, resources, roles and responsibilities required to prepare, respond, investigate and remediate any cybersecurity events or incidents within the Government.

GITSIR provides the appropriate coordination, technical assistance and advice on containment, eradication, recovery and investigation, as well as serves as the primary point of contact for all cybersecurity incidents in the Government. When necessary, GITSIR can be the contact point for agencies to escalate incidents to external Computer Security Incident Response teams (CSIRTs) and Internet Service Providers (ISPs).

GITSIR provides resources such as directives, advisories, instructions and playbooks, to prepare and guide agencies in addressing cybersecurity vulnerabilities and threats.

5.2. Communication and Authentication

To exchange secret or sensitive information, encrypted communication is mandated. SE3 encryption shall be used (refer to Paragraph 3.8.). A pre-established list of contacts (i.e. ACISO/SIRO) will be used for identity verification.

Official communication between agencies and GITSIR shall be through the GITSIR email account (refer to Paragraph 3.7.).

6. Services

6.1. Incident Response

Depending on the severity of the reported cybersecurity incident, agencies are expected to submit the incident report to Government Incident Reporting and Operation Centre (GIROC) within the timeframe stipulated within the WoG Cybersecurity IM SOP. Upon receipt of the escalated cybersecurity incidents, GITSIR will respond to agencies within 3 days to provide support comprising technical assistance and professional advice in the following aspects of incident management:

6.1.1. Incident Coordination and Triage

- Assess if the incident is cybersecurity related and prioritise based on incident severity
- Determine and advise on appropriate actions for affected agency to take
- Manage the implementation of WoG prevention measures

6.1.2. Incident Remediation and Investigation

- Provide Log Analysis, Digital Forensics and Malware Analysis support for compromised system (if required)
- Collect statistics and learning points from incidents that could help to prevent future attacks
- Issue directives, advisories, instructions and playbooks, to mitigate the risks and occurrences of future cybersecurity incidents

7. Incident Reporting Form

Government ICT and Data Incident Reporting Form described in ICT and Data Incident Reporting shall be used to report incident to GovTech.