Profile of GovCERT.HK

1. Document Information

This document provides a description of GovCERT.HK with reference to RFC 2350[1]. It provides basic information about the GovCERT.HK team, its channels of communication, roles, responsibilities and services.

1.1 Date of Last Update

This is version 1.4 as of 15th September 2020.

1.2 Distribution List for Notifications

Members of GovCERT.HK will be notified of updates of this document.

1.3 Location Where This Document May Be Found

The current version of this document is available on the GovCERT.HK website.

1.4 Authenticating This Document

This document has been signed with the PGP key of GovCERT.HK (see Section 2.6 below).

[1] https://www.ietf.org/rfc/rfc2350.txt

2. Contact Information

2.1 Name of the Team

Government Computer Emergency Response Team Hong Kong
Short name: GovCERT.HK

2.2 Address

GovCERT.HK
Level 6, Cyberport 1
100 Cyberport Road
Cyberport, Hong Kong

2.3 Time Zone

Hong Kong (GMT +08:00)

2.4 Facsimile Number

+852 2519 7320

2.5 Electronic Mail Address

All communications to GovCERT.HK should be sent to cert@govcert.gov.hk.

The Government of the Hong Kong Special Administrative Region of the People’s Republic of China (the Government) users should use the internal e-mail system to report all incidents.

2.6 Public Keys and Encryption Information

S/MIME is used for the transmission of sensitive data between GovCERT.HK and the constituency.

GovCERT.HK has a PGP key (key ID: 0x7D779220, fingerprint: 93A6 1508 500A 73F8 4817 9721 FA29 2F03 7D77 9220). The key can be found at the following websites and public key servers:

- the GovCERT.HK website (URL: www.govcert.gov.hk)
- the PGP.com key server (URL: keyserver.pgp.com)
- MIT PGP Public Key Server (URL: pgp.mit.edu)
- SKS OpenPGP Key server (URL: keys.gnupg.net)

2.7 Team Members

The GovCERT.HK team leader is the Chief Systems Manager (Project Governance and Cybersecurity) of the Digital Policy Office (DPO). The team is made up of IT security professionals from DPO.

2.8 Other Information

General information on GovCERT.HK is available on the www.govcert.gov.hk website.

2.9 Contact Points

The preferred method of contacting GovCERT.HK is via e-mail to cert@govcert.gov.hk. If urgent assistance is required, please include the keyword [URGENT] in your subject line.

3. Charter

3.1 Mission Statement

The mission of GovCERT.HK is to support the Government in information and cyber security.

The GovCERT.HK activities include disseminating alerts and warnings; issuing advisories on security measures; coordinating incident response and recovery; and promoting public awareness of and education on information security. GovCERT.HK will also engage the CERT community and vendors for effective responsiveness in case of incidents and exchanges of best practices with a view to strengthening the information and cyber security capability in the region.

3.2 Constituency

GovCERT.HK is a governmental CERT dedicated to coordinating information and cyber security incidents within the Government. The constituency of GovCERT.HK consists of all Government bureaux and departments (B/Ds).

3.3 Sponsorship and/or Affiliation

GovCERT.HK is a work unit established under the DPO. It is a national computer security incident response team (CSIRT) fully funded by the Government.

GovCERT.HK collaborates closely with Hong Kong Computer Emergency Response Coordination Centre (HKCERT) and engages other national CSIRTs through the CERT/CC, the Forum for Incident Response and Security Teams (FIRST), and the Asia Pacific Computer Emergency Response Team (APCERT).

3.4 Authority

GovCERT.HK operates under the auspices of the DPO to act as a governmental CERT for the Government.

4. Policies

4.1 Types of Incidents and Level of Support

GovCERT.HK properly coordinates resources for mitigating the impacts of security incidents at an appropriate support level depending on the type, severity and extent of the incidents as well as the order of priority as set out below:

1. Threat to human life and safety.
2. Compromise of sensitive or critical resources.
3. Compromise of important data which is costly when lost or damaged.
4. Damage to systems with costly downtime and recovery cost.
5. Disruption of service.
6. Loss of public image of the B/D or the Government as a whole.

4.2 Co-operation, Interaction and Disclosure of Information

GovCERT.HK works in cooperation with local law enforcement agencies, other CERTs and organisations in sharing information on security alerts and threats. GovCERT.HK follows the Traffic Light Protocol (TLP) for the exchange of sensitive information with other CERTs or organisations.

Security incident information and certain system vulnerability information are handled as RESTRICTED information within the GovCERT.HK. Such information can only be exchanged and transferred among authorised members of GovCERT.HK team, staff members responsible for the security of the affected information systems, and investigators who involve in the forensic investigations. Lessons learnt would be shared with the constituency and the CERT community.

4.3 Communication and Authentication

GovCERT.HK protects sensitive information in accordance with relevant regulations and policies within the Government.

Transmission of sensitive information is encrypted and signed using either S/MIME or PGP.

5. Services

5.1 Incident Response

GovCERT.HK will assist B/Ds in handling the technical aspects of security incidents. In particular, it will provide assistance and advice with regard to the following aspects of security incident management:

5.1.1 Incident Triage

- Assess the extent and impact of security incidents arisen within the Government.

5.1.2 Incident Coordination

- Coordinate and advise on the handling of security incidents within the Government.
- Coordinate with the stakeholders concerned to step up measures against alleged and real cyber attacks.

5.1.3 Incident Resolution

- Give advice or assistance to the B/Ds concerned on appropriate actions to contain the damages of security incidents if necessary.
- Follow up with the B/Ds concerned on the progress of security incident handling process.

5.2 Proactive Activities

GovCERT.HK coordinates and maintains the following services:

- Disseminate security alerts, advisories and related information;
- Promote security awareness to the Government and the public through seminars and trainings;
- Coordinate preventive vulnerability scanning and cyber security drills; and
- Collaborate with relevant institutions to share latest security threats and information.

6. Incident Reporting Forms

The sample Preliminary Information Security Incident Reporting Form and Post Incident Report, for reference of the constituency, are documented in the Practice Guide for Information Security Incident Handling (ISPG-SM02) and available on this website and intranet.

7. Disclaimers

While every precaution is taken in the preparation of information, notifications and alerts, GovCERT.HK assumes no responsibility for errors and omissions, or for damages resulting from the use of the information contained therein.

ENDS