Detailed information (RFC 2350)

SIGOV-CERT RFC 2350

1 Document Information

This document describes SIGOV-CERT in accordance with RFC 2350.

1.1 Date of Last Update

Version 1.0, published on 31st Januar 2019.

1.2 Distribution List for Notifications

Changes to this document are not distributed by a mailing list.

1.3 Locations where this Document May Be Found

The document is located at the following address:

http://www.mju.gov.si/en/areas_of_work/information_and_communications_technology/

The latest version is available also upon request to cert(at)gov.si via electronic mail.

2 Contact Information

2.1 Name of the Team

SIGOV-CERT: Slovenian Governmental Computer Emergency Response Team (English name)

SIGOV-CERT: Odzivni center za incidente v informacijskih sistemih državne uprave (Slovenian name)

2.2 Address

SIGOV-CERT
Ministrstvo za javno upravo

Tržaška c. 21,
SI-1000 Ljubljana
Slovenia

2.3 Time Zone

- CET, Central European Time
  (UTC+1, between last Sunday in October and last Sunday in March)
- CEST (also CET DST), Central European Summer Time
  (UTC+2, between last Sunday in March and last Sunday in October)

2.4 Telephone Number

+386 1 478 86 51

2.5 Facsimile Number

+386 1 478 86 49

2.6 Other Telecommunication

None.

2.7 Electronic Mail Address

cert(at)gov.si

2.8 Public Keys and Encryption Information

SIGOV-CERT uses PGP for digital signatures and to receive encrypted information. The key is available on PGP/GPG keyservers:
http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/Direktorat_za_informatiko/sigov-cert-pgp.asc.asc

Information about the key:

pub rsa4096 2019-01-24 [SCA] [expires: 2024-01-24]
Key fingerprint = 3002 991D C8A4 3CB3 2D57 16F0 EDBD E956 865C 503B
uid SIGOV-CERT <SIGOV-CERT(at)gov.si>
uid SIGOV-CERT <cert(at)gov.si>

2.9 Team Members

Damjan Križman is the Team Manager of SIGOV-CERT. A full list of other members of SIGOV-CERT is not publicly available. Team members will identify themselves to the reporting party with their full name in an official communication regarding an incident.

2.10 Other Information

General information about SIGOV-CERT in English language is available at http://www.mju.gov.si/en/areas_of_work/information_and_communications_technology/. Information in Slovenian language including SIGOV-CERT news and bulletins is available at http://www.mju.gov.si/si/delovna_podrocja/informatika/informacijska_varnost/.

2.11 Points of Customer Contact

The preferred method of contacting SIGOV-CERT is via e-mail at cert(at)gov.si. Office hours for SIGOV-CERT are between 8:00 and 16:00 on working days. During office hours, SIGOV-CERT staff is available via telephone. Outside office hours team member on duty regularly checks for reports directed to the mentioned e-mail address.

3 Charter

3.1 Mission Statement

SIGOV-CERT offers assistance in computer and network security incident handling and provides incident coordination functions for all incidents involving systems and networks under management of Ministry of Public Administration of Republic of Slovenia. SIGOV-CERT helps raising awareness on issues of network and information security and provides advisories and alerts to the state public servants.

3.2 Constituency

SIGOV-CERT is the Slovenian Governmental CERT and its constituency includes all networks, information systems and users of those systems managed by Ministry of Public Administration of Republic of Slovenia.

3.3 Sponsorship and/or Affiliation

SIGOV-CERT operates within IT Services Directorate, Information security sector at the Ministry of Public Administration of Republic of Slovenia.

3.4 Authority

SIGOV-CERT operates with the authority of Ministry of Public Administration of Republic of Slovenia as its parent organization. SIGOV-CERT strives to maintain active cooperation and partnerships with all Slovenian ISPs, law-enforcement bodies and other stakeholders in the field of network and information security.

4 Policies

4.1 Types of Incidents and Level of Support

SIGOV-CERT handles various types of security incidents that occur on networks or information systems operated by IT Services Directorate at the Ministry of Public Administration of Republic of Slovenia. The level of support depends on the type of the incident and the severity as determined by SIGOV-CERT staff.

4.2 Co-operation, Interaction and Disclosure of Information

SIGOV-CERT treats all information included in the correspondence as confidential. Information will only be disclosed to other parties involved in the investigation of the reported incident. In such events any identifiable information that is not crucial to the investigation by the party involved will be anonymised.

SIGOV-CERT discloses information to other bodies only in accordance with applicable Slovenian legislation.

4.3 Communication and Authentication

The preferred method of communication is via e-mail. When the content is deemed sensitive enough or requires authentication, SIGOV-CERT PGP key is used for signing e-mail messages. All sensitive communication to SIGOV-CERT should be encrypted by the team's PGP key. Alternative methods can be agreed on over the phone.

5 Services

5.1 Incident Response

SIGOV-CERT will assist anyone within the constituency in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1. Incident Triage

- Investigating whether indeed an incident occurred.
- Determining the extent of the incident.

5.1.2. Incident Coordination

- Determining the initial cause of the incident.
- Facilitating contact with other users or system administrators which may be involved.
- Making reports to other CERT/CSIRTs.
- Composing announcements to users, when applicable.

5.1.3. Incident Resolution

- Providing advice to the reporting party that will help removing the vulnerabilities that caused the incident and securing the systems from the effects of the incidents.
- Evaluating which actions are most suitable to provide desired results regarding the incident resolution.
- Provide assistance in evidence collection and data interpretation when needed.

5.2 Proactive Activities

Within

- **Awareness-raising program**
  SIGOV-CERT is running the Governmental awareness-raising program targeted at state's public servants users. Goals of the program are to provide efficient methods for risk identification and mitigation and to raise awareness.
- **Information services**
  SIGOV-CERT publishes advisories for events and incidents that are considered of special importance to users in the constituency. Information is disseminated via various channels (web, mailing lists).
- **Training services**
  SIGOV-CERT members give periodic lectures, seminars and workshops on network and information security topics.

6 Incident Reporting Forms

Reports are normally sent to the e-mail address cert@gov.si, for users in Governmental network service desk tool shall be used.

.

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, SIGOV-CERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.