RFC2350 – GOVCERT.RS

1. Information about the document

This document contains information about GOVCERT.RS.

1.1Last modified date

27.05.2024.

1.2Distribution list for notifications

There is no distribution list for notifications of changes to this document

1.3Document availability locations

The last version of this document is available at

https://www.ite.gov.rs/tekst/en/27/cert.php

2. Contact information

2.1Name of the team

Short name: GOVCERT.RS
Long name: (Office for IT and eGovernment Computer Emergency Response Team of the Republic of Serbia)

2.2Address

Nemanjina 11, Beograd, 11000, Serbia

2.3Time 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)

2.4Phone number:

+ 381 11 7358 400

2.5Fax number

None available.

2.6Other contact methods

None available.

2.7E-mail address

cert@gov.rs

2.8Public keys and encryption information

GOVCERT.RS uses PGP for digital signatures and to receive encrypted information. The key is available on PGP/GPG keyservers and at:
Key Fingerprint= 27669C7FFC5B64396F84E47418244C141B54747D

2.9Team members

Members of the GOVCERT.RS-a will identify themselves upon entering into communication.

2.10 Other information

All information about GOVCERT.RS-u is available at:
https://www.ite.gov.rs/tekst/en/27/cert.php

2.11 Preferred methods of communication

Primary communication method is by using email at cert@gov.rs, secondary method is via phone +381 11 7358 400.

3. Charter

3.1Mission

The main task of the GOVCERT.RS (the CSIRT of government authorities) is to ensure the information security of the ICT infrastructure, the Office services and the confidentiality, integrity and availability of information systems and network. This requires effective incident response in a timely manner when they occur, preventive activities to minimize the number of possible incidents and raising awareness of ICT security among government authorities.

3.2Constituencys

GOVCERT.RS - performs tasks related to protection against incidents in the system of the republican institutions in the unified information and communication network of electronic administration.

3.3Sponsorship or affiliation

GOVCERT.RS is located within the Government Office for Information Technologies and Electronic Administration, which is responsible for designing, development, construction, maintenance and improvement of the unique information and communication network of electronic administration.

3.4Authority

The Center for the Security Information and communcation systems of institutions (GOVCERT.RS) was established (Information security Law, ''Official gazette of the Republic of Serbia'', No. 6/2016 and 94/2017) within the Office for Information Technologies and Electronic Administration responsible for designing, development, construction, maintenance and improvement of the unique information and communication network of electronic administration (Law on electronic administration, ''Official gazette of the Republic of Serbia'', No. 27/2018):

4. Policies

4.1Incident types and support levels

During the incident response GOVCERT.RS responds to all types of incidents and has a coordination role within the constituency in order to carry out those activities needed to make the right decisions from detection to resolution of the incident. All other services such as vulnerability detection, monitoring and detection by the SOC team, coordination with other organizations and notification and education are performed by OITeG CERT entirely for the purpose of protecting and improving the security of the systems of republic institutions and organizations.

4.2Collaboration, interaction and information sharing

GOVCERT.RS takes privacy very seriously so any shared data will be shared without personal or sensitive information. The data may be shared by GOVCERT.RS is statistical.

GOVCERT.RS uses TLPv2. More information about TLPv2 is used at https://www.ite.gov.rs/extfile/en/849/TLP.docx

4.3Communication and authentication

GOVCERT.RS considers all communication highly confidential. Wherever sensitive data is shared via email, PGP/GPG should be used, while non-sensitive information can be shared without encryption.

Telephone communication is considered safe for sharing all the information.

5. Services

5.1Reactive services

- Responding to security incidents;
- Responding to security vulnerabilities and failures ;
- Alerts about observed incidents and vulnerabilities.

5.2Proactive services

- Used technologies monitoring;
- Conducting security audits and assessment of the Office's systems and services;
- Configuring and maintaining security tools;
- System intrusion detection;
- Publication of new information and news of importance for information security;
- Knowledge dissemination to state authorities related to information security;
- Conducting security audits and assessments .

5.3Safety quality management field services

- Risk analysis;
- Ensuring continuous operations where incidents occur;
- Raising the level of information security awareness;
- Employee education.

6. Incident report form

Incident report form is available at https://www.ite.gov.rs/tekst/en/27/cert.php

7. Disclaimer

GOVCERT.RS takes all steps to ensure the correctness of the information it shares, but assumes no responsibilities for any damage caused by their use.