**RFC2350**

1. **Information about the document**

This document containes information about GOVCERT.RS

* 1. **Last modified date**

17.06.2023.

* 1. **Distribution list for notifications**

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

* 1. **Document availability locations**

The last version of this document is available at

<https://www.ite.gov.rs/tekst/sr/88/cert.php>

1. **Contact informations**
   1. **Name of the CSIRT team**

GOVCERT.RS (Office for IT and eGovernment Computer Emergency Response Team)

* 1. **Address**

Nemanjina 11, Beograd, 11000, Srbija

* 1. **Time zone**

CET; UTC+01:00

* 1. **Phone number:**

+ 381 11 7358 400

* 1. **Fax number**

/

* 1. **Other contact methods**

Do not exist

**2.7 E-mail address**

[cert@gov.rs](mailto:cert@gov.rs)

* 1. **Public keys and encription information**

Key Fingerprint= 27669C7FFC5B64396F84E47418244C141B54747D

* 1. **Team members**

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

* 1. **Other information**

All information about GOVCERT.RS -u are available at: <https://www.ite.gov.rs/tekst/sr/88/cert.php>

* 1. **Preferred methods of communication**

Primary comunication method is by using email-a through [cert@gov.rs](mailto:cert@gov.rs), and secondary method is via phone +381 11 7358 400

1. **Charter** 
   1. **Mission**

The main task of the CERT of the republic authorities is to ensure the information security of the ICT infrastructure, the Office services and the unique information and communication network of electronic administration. This includes effective response and incident resolution when they occur, preventive activities to minimize the number of possible incidents and raising awareness of ICT security among government authorities.

* 1. **Constituens**

The CERT of the republican institutions performs tasks related to protection against incidents in the system of the republican institutions in the unified information and communication network of electronic administation

* 1. **Sponsorship or affiliation**

GOVCERT.RS is located 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.

* 1. **Jurisdiction**

The Center for the Security Information and communcation systems of institutions (CERT of republic institutions) 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):

1. **Politics**
   1. **Incident types and support levels**

During the incident response GOVCERT.RS responds to all types of incidents and has a coordination role 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 GOVCERT.RS entirely for the purpose of protecting and improving the security of the systems of republic institutions and organizations.

* 1. **Collaboration, 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.

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

* 1. **Communication 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.

1. **Services** 
   1. **Reactive services**

* Responding to security incidents;
* Responding to security vulnerabilities and failures ;
* Alerts about observed incidents and vulnerabilities.
  1. **Proactive services**
* Used technologies monitoring;
* Conducting a security audits and assesments of the Office’s systems and services;
* Configuring and mainting 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 a security audits and assessments .
  1. **Safety quality management field services**
* Risk analyses;
* Ensuring continuous operations where incidents occur;
* Raising the level of information security awareness;
* Employee education.

1. **Incident report form**

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

1. **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.