RFC 2350 description for ICT-CERT

1. About this document

This document contains a description for the Critical Information and Infrastructure Protection ICT-CERT of Republic of Kosovo according to RFC 2350. It provides basic information about the CERT, the way how it can be contacted, describes its responsibilities and the services offered.

1.1. Date of Last Update

This is version 0.1 of 27/11/2018.

1.2. Distribution List for Notifications

There is no distribution list for notifications. Any specific questions or remarks please address to the ICT-CERT mail address info@academyict.net

1.3. Location where this Document may be found

The current version of this CERT description documents is available from the Academy ICT website https://academyict.net/ict-cert/

2. Contact Information

2.1. Name of the Team

ICT-CERT, Critical Information and Infrastructure Protection Kosovo.

2.2. Address

Academy ICT for Professional Expertise

CERT division

10000 Pristina,

Republic of Kosovo

2.3. Time Zone

GMT, Greenwich Mean Time
(GMT+01, from the last Sunday in October to the last Saturday in March)

GMT, Greenwich Mean Time
(GMT+02, from the last Sunday in March to the last Saturday in October)

2.4. Telephone Number

Mob: +383 49 459 572

2.5. Other Telecommunication

None available

2.6. Electronic Mail Address

For the incident reports and non-incident, please use the address info@academyict.net

2.7. Public Keys and Encryption Information

For the incident and non-incident related communication, you can use this key:

2.8. Team Members

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

Management, liaison and supervision are provided by Atdhe Buja, CEO, of Academy ICT.

2.9. Other information

General information about the ICT-CERT can be found at https://academyict.net/ict-cert/

2.10. Points of Customer Contact

The preferred method for contacting ICT-CERT is via e-mail. Incident reports and related issues should be sent to the address info@academyict.net .This will create a ticket in our tracking system and alert the human on duty. For general questions please send an e-mail to info@academyict.net

If it is not possible (or not advisable for security reasons) to use e-mail, the ICT-CERT can be reached by telephone at +383 49 459 572.

The ICT-CERT's hours of operation are generally restricted to regular business hours (08:00-18:00 Monday to Friday except holidays).

3. Charter

3.1. Mission

In accordance with Academy ICT regulations, mission of ICT-CERT is to identify, protect & solve cyber security actual & future challenges with a main focus on Critical Information and Infrastructure protection.

3.2. Constituency

Our constituency is in critical IT businesses; mainly focus on Critical Information Protection and/or Critical Information and Infrastructure protection.

3.3. Sponsorship and/or Affiliation

ICT-CERT is functional Division within Academy ICT.

3.4. Authority

The ICT-CERT Division operates under the document Strategy for Cyber Security & Protection of Privacy for ICT-CERT. Operates by respecting legislation of Republic of Kosovo.

The ICT-CERT expects to work cooperatively with industry, system administrators and users of Academy ICT, public and private sector in Republic of Kosovo also international parties.

4. Policies

4.1. Type of Incidents and Level of Support

The ICT-CERT Division is authorized to address all types of computer security incidents which occur, or threaten to occur, in our constituency.

The level of support given by ICT-CERT will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and ICT-CERT's resources at the time, though in all cases some response will be made within one working day.

Note that direct support will be given to end users; also they are expected to contact their system administrator, network administrator or their ISP for assistance.

ICT-CERT is committed to keeping its constituency informed of potential vulnerabilities, and where possible, will inform this community of such vulnerabilities before they are actively exploited.

4.2. Co-operation, Interaction and Disclosure of Information

All incoming information is handled confidentially by ICT-CERT, regardless of its priority. Information that is evidently very sensitive in nature is only communicated and stored in a secure environment, if necessary using encryption technologies.

ICT-CERT will use the information you provide to help incident response coordination. Information will only be distributed further to other teams and members on a need-to-know base, and preferably in an anonymized fashion.

The ICT-CERT operates by respecting legislation of Republic of Kosovo.

4.3. Communication and Authentication

E-mails and telephones are considered sufficiently secure to be used even unencrypted for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP will be used.

If it is necessary to authenticate a person before communicating, this can be done either through existing webs of trust (e.g. TI, FIRST) or by other methods like call-back, mail-back or even face-to-face meeting if necessary.

5. Services

5.1. Incident response coordination

Part of the coordination work may involve notification and collaboration with law enforcement agencies and other local and national CERTs with the focus protection of information system, users of electronic communication networks and services, a list of services provided by ICT-CERT Division is here https://academyict.net/ict-cert/

5.2. Awareness Building

Performing this service seek opportunities to increase security awareness through developing articles, posters, newsletters, web sites, or other informational resources that explain security best practices and provide advice on precautions to take. Activities may also include scheduling meetings and seminars to keep constituents up to date with ongoing security procedures and potential threats to organizational systems.

6. Disclaimer

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