**Republika e Kosovës**
Republika Kosova-Republic of Kosovo
Qeveria–Vlada–Government
Ministria e Digjitalizimit dhe Administratës Publike
*Ministry of Digitalization and Public Administration - Ministarstvo Digitalizacije i Javne Uprave*
Agjencia e Shoqërisë së Informacionit
*Agencija za Informaciono Društvo - Agency of Information Society*

---

# RFC 2350 Description for Kosovo Government CERT (GovCERT XK)

## 1. About this Document

This document contains a description of the Kosovo Government CERT (GovCERT XK) in accordance with RFC 2350. It provides basic information about the team, the ways it can be contacted, describes its responsibilities, and the services offered.

The full text of RFC 2350 – Expectations for Computer Security Incident Response – is available at:

https://www.ietf.org/rfc/rfc2350.txt

### 1.1 Date of Last Update

This is version 1.0, published 06 August 2026.

### 1.2 Distribution List for Notifications

This document is publicly available. There is no distribution list for notifications of changes to this document. Questions or remarks regarding this document should be addressed to the GovCERT XK e-mail address (see Section 2.6).

### 1.3 Locations where this Document May Be Found

The current version of this document is available at:

Official website: https://govcert.rks-gov.net

Trusted Introducer: https://www.trusted-introducer.org

# 2. Contact Information

## 2.1 Name of the Team

Kosovo Government CERT (Short name: GovCERT XK)

## 2.2 Address

Kosovo Government CERT

Agency for Information Society (ASHI)

“Luan Haradinaj” Street, Rilindja Building

10000 Prishtina

Republic of Kosovo

## 2.3 Time Zone

Central European Time, CET (UTC+01:00, from the last Sunday in October to the last Sunday in March)

Central European Summer Time, CEST (UTC+02:00, from the last Sunday in March to the last Sunday in October)

## 2.4 Telephone Number

+383 38 200 60112 ; +38344211969

## 2.5 Facsimile Number

None available.

## 2.6 Electronic Mail Address

For incident reports and general enquiries, please use: ashi.cert@rks-gov.net and gani.zogaj@rks-gov.net

## 2.7 Public Keys and Encryption Information

GovCERT XK operates PGP keys for secure communication, associated with the following e-mail addresses:

**Email: gani.zogaj@rks-gov.net**

Key ID: 5C0B5EB8B107DFD0

Fingerprint: AFDB 08D3 E047 CC6E 8891 00DB 5C0B 5EB8 B107 DFD0

**Email: ashi.cert@rks-gov.net**

Key ID: 59DAD637058EF0B5 (EdDSA/255)

Fingerprint: AB9E 1FDE 3161 32FE D5E8 1C46 59DA D637 058E F0B5

The key(s) can be found at: https://govcert.rks-gov.net First key for ashi.cert@rks-gov.net expire 2028-06-23, second  key expire 2029-11-19 and will be renewed prior to expiry.

### 2.8 Team Members

GovCERT XK is part of the Agency for Information Society (ASHI). Point of contact: Gani Zogaj. A full list of team members is not publicly disclosed. Staff will identify themselves by full name in official communication regarding an incident.

### 2.9 Other Information

General information about GovCERT XK and ASHI can be found at: https://govcert.rks-gov.net

### 2.10 Points of Customer Contact

The preferred method of contacting GovCERT XK is via e-mail, as described in Section 2.6. This will create a ticket in the team's tracking system and alert the analyst on duty.

If e-mail is not available, or not advisable for security reasons, GovCERT XK may be reached by telephone at +383 38 200 60112 and +38344211969.

GovCERT XK's regular hours of operation are 08:00–16:00, Monday to Friday, excluding public holidays in the Republic of Kosovo.

## 3. Charter

### 3.1 Mission Statement

Kosovo Government CERT (GovCERT XK) plays a key role in safeguarding the information systems, electronic communication networks and services of Kosovo government institutions. Its goal is to help constituents effectively face cyber security challenges, and to coordinate the prevention, detection, and resolution of security incidents.

### 3.2 Constituency

GovCERT XK provides cybersecurity incident response, coordination, prevention, and advisory services to central government institutions, government agencies, and other public sector entities operating under the Government of the Republic of Kosovo. The constituency includes government information systems, networks, and critical digital services under its mandate, including but not limited to:

- ASN 213206
- Domain: rks-gov.net
- IP range: 91.239.145.0/24

### 3.3 Sponsorship and/or Affiliation

GovCERT XK is a functional unit of the Agency for Information Society (ASHI), established on 14 February 2019. Agency for Information Society itself was established under Law No. 04/L-145 on Government Bodies for the Information Society (published 15 May 2013).

### 3.4 Authority

GovCERT XK operates under the authority delegated to it by the Government of the Republic of Kosovo, and within the bounds of applicable Kosovo legislation, in particular:

- Law No. 08/L-173 on Cyber Security (published 27 February 2023, Official Gazette No. 4/2023);
- Law No. 04/L-145 on Government Bodies for the Information Society (published 15 May 2013, Official Gazette No. 15/2013).

GovCERT XK expects to work cooperatively with system administrators and users within its constituency, and does not exercise authority beyond its constituency.

# 4. Policies

## 4.1 Types of Incidents and Level of Support

GovCERT XK is authorised to address all types of computer security incidents which occur, or threaten to occur, within its constituency.

The level of support provided will vary depending on the type and severity of the incident, the type of constituent affected, the size of the community impacted, and GovCERT XK's resources at the time – though in all cases an initial response will be made within one working day.

End users are expected to contact their own system or network administrator, or their institution's IT department, for direct assistance; GovCERT XK supports these intermediaries rather than individual end users directly.

## 4.2 Information Classification

GovCERT XK classifies and handles information it receives or produces according to the Traffic Light Protocol (TLP). This classification determines the audience with which information may be shared:

| Classification Level | Description |
|---|---|
| **TLP:RED** | For the eyes and ears of individual recipients only, no further disclosure. Not for sharing beyond the specific exchange or meeting in which it was originally shared. |
| **TLP:AMBER** | Limited disclosure. Recipients may share TLP:AMBER information only with members of their own organisation and with clients or constituents who need to know the information to protect themselves or prevent further harm. |
| **TLP:GREEN** | Limited disclosure. Recipients may share TLP:GREEN information with peers and partner organisations within their sector or community, but not via publicly accessible channels. |
| **TLP:CLEAR** | Recipients may share this information without restriction, subject to standard copyright rules. |

## 4.3 Information Disclosure and Exclusivity

Exclusivity, in this context, defines who has access to which category of information handled by GovCERT XK, and under what conditions it may be further shared.

All information received by GovCERT XK is handled confidentially, regardless of its classification level. Information that is evidently sensitive is communicated and stored only in a secure environment, using encryption where necessary.

Information is shared further only in accordance with its assigned classification level (see Section 4.2), on a strict need-to-know basis, and – where possible – in anonymised form. Information marked TLP:RED or TLP:AMBER is shared only with the specific recipients, organisation, or constituents designated by the classification, and never distributed beyond that group without the originator's explicit consent.

GovCERT XK operates within the bounds of the legislation of the Republic of Kosovo, and may be required to disclose information to competent national authorities pursuant to that legislation.

### 4.4 Communication and Authentication

E-mail and telephone are considered sufficiently secure for the transmission of low-sensitivity (TLP:CLEAR / TLP:GREEN) data, even unencrypted. Where it is necessary to send highly sensitive data (TLP:AMBER / TLP:RED) by e-mail, PGP encryption will be used (see Section 2.7).

Where it is necessary to authenticate a person before communicating, this may be done through existing webs of trust (e.g. Trusted Introducer, FIRST), or by other methods such as call-back, mail-back, or a face-to-face meeting.

## 5. Services

### 5.1 Incident Response Coordination

GovCERT XK coordinates the response effort among constituents involved in an incident. This may include collecting contact information, notifying sites of potential involvement (as victim or source of an attack), collecting statistics, and facilitating information exchange, including with law enforcement and other national and international CERTs.

This service does not include direct, on-site incident response.

### 5.2 Proactive Services

GovCERT XK prepares security alerts and advisories for its constituency, including timely information on current threats and vulnerabilities relevant to government networks and systems.

### 5.3 Awareness Building

GovCERT XK seeks to increase security awareness across its constituency through advisories, guidance materials, and where appropriate, briefings and training sessions, to keep constituents informed of current best practices and emerging threats.

## 6. Incident Reporting Forms

An incident reporting form is available at:ashi.cert@rks-gov.net Where a form is not available, incidents may be reported directly by e-mail to the address in Section 2.6.

## 7. Disclaimers

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

# 8. Trusted Introducer Accreditation Status

GovCERT XK is registered with Trusted Introducer (TF-CSIRT), the trusted backbone of the security and incident response community in Europe. The information below reflects the team's current standing in the Trusted Introducer Directory and is updated as the accreditation process progresses.

## 8.1 Current Status

- Current State: Accreditation Candidate
- Entry Date (Listed): 16 July 2025
- Accreditation Candidate since: 14 July 2026
- Last Change: 23 July 2026
- Date of Accreditation: pending

## 8.2 History

| Date | Description |
|---|---|
| 14 Jul 2026 | GovCERT XK is registered as an Accreditation Candidate team with Trusted Introducer. |
| 16 Jul 2025 | GovCERT XK is registered as a Listed team with Trusted Introducer. |

Further information about the Trusted Introducer accreditation framework and the current listing for GovCERT XK is available at:
https://www.trusted-introducer.org