AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

RFC 2350 description for AKSK

(National Cyber Security Authority)

Autoriteti Kombëtar për Sigurine Kibernetike

Rruga. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Shqipëri 04-22-21039
Email:info@aksk.gov.al
Web:www.aksk.gov.al

Contents

1. About this document

This document contains a description for the National CSIRT of the Republic of Albania according to RFC 2350. It provides basic information about the CSIRT, the ways it can be contacted and describes its responsibilities and the services offered.

1.1 Date of Last Update

This is version 3 of 09/03/2026

1.2 Distribution List for Notifications

There is a distribution list for notifications only for the CII point of contacts in the Republic of Albania. Any other specific questions or remarks please address the AKSK mail address.

1.3 Locations Where This Document May Be Found

The current version of this CIRT description document is available from the AKSK website – https://aksk.gov.al/rreth-nesh/

2. Contact Information

2.1 Name of the Team

AKSK, Autoriteti Kombëtar për Sigurinë Kibernetike

2.2 Address

Autoriteti Kombëtar për Sigurinë Kibernetike

Rruga: “Papa Gjon Pali II”, Nr 3, Kati I, Tiranë, Shqipëri

2.3 Time Zone

CET, Central European Time (UTC+1, from the last Sunday in October to the last Saturday in March) CEST, Central European Summer Time (UTC+2, from the last Sunday in March to the last Saturday in October)

2.4 Telephone Number

+355-(0) 422 21 039

2.5 Facsimile Number

+355-(0) 422 21 039

2.6 Other Telecommunication

Not available

2.7 Electronic Mail Address

For the incident reports, please use the address soc@aksk.gov.al

For illegal and harmful content online reports can be submitted at https://aksk.gov.al/raporto-5/, raporto@aksk.gov.al

2.8 Public Keys and Encryption Information

For incident related communication, you can use this key:

User ID: Info AKSK, info@aksk.gov.al

Valid From: 03/09/2026

Valid Until: 03/09/2029

Status: Certified

-----BEGIN PGP PUBLIC KEY BLOCK-----

mDMEaa7i7hYJKwYBBAHaRw8BAQdAFA/le0aRTkrTgvj+tnd0Gwlfu3QuW1nllBEe
DBZ5QlC0HEluZm8gQUtTSyA8aW5mb0Bha3NrLmdvdi5hbD6ImQQTFgoAQRYhBEu8
qfXu8iaiidC27jPLCdPSHtT2BQJpruLuAhsDBQkFpLFCBQsJCAcCAiICBhUKCQgL
AgQWAgMBAh4HAheAAAoJEDPLCdPSHtT2SmkA/2W9DZq0NYT+mGr1OKc31JuJrf/C
GoPLZ7fKwJN1g/qVAQCUpijLwPjf8PQwkrgyv3a3mlH6XKoQALD485jVy5JuBbg4
BGmu4u4SCisGAQQBl1UBBQEBB0AgLV/vzVtjBR4kASQMiCXb45JN4cddZ7PsFLNk
a8yuFwMBCAeIfgQYFgoAJhYhBEu8qfXu8iaiidC27jPLCdPSHtT2BQJpruLuAhsM
BQkFpLFCAAoJEDPLCdPSHtT20CQA/1A+Ij99hRl+L3ei/sehL37RGDm565GmVSYA
Eqe0hD9xAQCS2kmltOz7cKyc5eVNh7jn2ccU557nxPnf/9q64KNGAg==
=yKNE
-----END PGP PUBLIC KEY BLOCK-----

2.9 Team Members

AKSK consists of six (6 directories) with respective units committed to increasing cybersecurity levels in the Republic of Albania:

- Directorate Of Certification, Policies & Cyber Security Legislation –Mrs. Irma Droboniku
- Directorate of International Coordination Projects and Strategic Development of Cyber Security – Mrs. Floreta Faber
- Directorate of Cyber Security Analysis – Mr. Adriano Lleshi
- Directorate of Monitoring and Incident Response, Operations Center Soc C-Sirt – Mrs. Esmeralda Kazia
- Directorate of Compliance Analysis, Risk and Control of Cyber Security Measures – Mr. Saimir Kapllani
- Directorate of Finance and Support Services- Mrs. Arlinda Drenofci

A full list of AKSK team members is not publicly available. Team members will identify with the reporting party with their full name in an official communication regarding an incident. General Management, liaison and supervision are provided by *Mr. Saimir Kapllani, Acting General Director, National Cyber Security Authority.*

2.10 Other Information

General information about the AKSK can be found at www.aksk.gov.al

2.11 Points of Customer Contact

The preferred method for contacting AKSK for all the issues related to incidents on CII is through internal portal issued by AKSK. For all other entities is via official email raporto@aksk.gov.al

For general questions please send an e-mail to info@aksk.gov.al . If it is not possible (or not advisable for security reasons) to use e-mail, AKSK can be reached by telephone at + 355 (0)422-21-039. The AKSK hours of operation are generally restricted to regular business hours (08:00-16:30 Monday to Friday except holidays).

3. Charter

3.1 Mission Statement

Achieving a high level of cybersecurity involves defining the necessary security measures, rights and obligations of relevant entities, as well as promoting cooperation among actors operating in this field.

This approach ensures reliability and security in electronic transactions between citizens, businesses and public authorities, contributing to the increased effectiveness of public and private services, as well as electronic commerce. Furthermore, it establishes minimum technical standards for data security and information networks/systems, in alignment with international standards, with the aim of creating a safe and trustworthy electronic environment.

3.2 Constituency

Our constituencies are stated by Law on Cyber Security No.25/2024 and defined by DCM No. 553, dated 15.07.2020, “On approval of the list of critical information infrastructures and list of important information infrastructures “(Updated by DCM Nr. 364 dated 30.06.2025)

3.3 Sponsorship and/or Affiliation

AKSK is an Authority under the Prime Minister’s Office which is financed by the state budget and other legal sources.

3.4 Authority

The National Cyber Security Authority operates under the authority of Law on Cybersecurity No. 25/2024. AKSK operates within the bounds of the Republic of Albania.

AKSK works cooperatively with CII operators of the Republic of Albania, public and private sectors as well as International Institutions which focus on Cyber Security

4. Policies

4.1 Types of Incidents and Level of Support

AKSK handles cybersecurity incidents in accordance with the Regulation on the Categorization of Cybersecurity Incidents (Approved by Order No. 299, dated 21.08.2024), which is publicly available at:
https://aksk.gov.al/wp-content/uploads/2024/08/Kategorizimi-i-incidenteve-te-sigurise-kibernetike-21.08.2024.pdf
Incidents are categorized based on their nature, severity, and impact on critical information infrastructure (CII). AKSK provides support according to the priority level of each incident, ensuring a coordinated and timely response. The level of support offered by AKSK may vary depending on the type and severity of the incident. AKSK reserves the right to determine the level of support provided in each case, based on available resources and the potential impact on national cybersecurity.

4.2 Co-operation, Interaction and Disclosure of Information

All incoming information is handled confidentially by AKSK, 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.

AKSK will use the information you provide to help with 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. For all cybersecurity incident information TLP protocol is applied.

AKSK operates within the bounds of the Republic of Albania's legislation.

4.3 Communication and Authentication

For all CII's operating in the Republic of Albania and identified by DCM Nr. 364 dated 30.06.2025 communication is done through internal system managed by AKSK.

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 meetings if necessary.

5. Services

5.1 Incident response coordination

AKSK coordinates the response effort among constituencies involved in the incident. This includes CII operators stated by DCM Nr. 364 dated 30.06.2025 of Republic of Albania. The coordination work may involve collecting contact information, notifying sites of their potential involvement (as victim or source of an attack), collecting statistics about the number of sites involved, and facilitating information exchange.

Part of the coordination work may involve notification and collaboration with law enforcement agencies and other local and national CSIRTs with the focus protection of CII systems, networks and services.

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

5.2 Awareness Building

AKSK Unit will prepare security alerts including:

- Safety warnings for specific needs of the constituency. These alerts provide timely information on the current situation and the activities that pose a threat to operators of electronic communication networks and services and their users.
- Safety warnings for the public. These alerts contain brief information that is clear for understanding from home computers user, to protect themselves from the internet.

Performing this service seeks 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. Incident Reporting Forms

The form is available on the following Kategorizimi-i-incidenteve-te-sigurise-kibernetike-21.08.2024.pdf Page 16.

7. Disclaimers

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