Republic of North Macedonia

Ministry of Digital Transformation

RFC2350

1. Overview

1.1. Introduction

This document describes the organization, responsibilities, services, and operating procedures of the Computer Incident Response Team for the executive authorities (MKD-GOV-CSIRT), which operates within the Ministry of Digital Transformation.

MKD-GOV-CSIRT acts upon reported or identified cybersecurity incidents affecting the network and information systems of the Government, ministries, independent state administration bodies, state administration bodies within ministries, administrative organizations, municipalities, municipalities within the City of Skopje, and the City of Skopje, with the aim of ensuring timely detection, analysis, coordination, and mitigation of the consequences of computer and network incidents.

The document is structured into several sections, each providing clear guidance and procedures for the proper and timely reporting of computer incidents to MKD-GOV-CSIRT, as well as information regarding communication and cooperation with the team.

1.2. Purpose

The purpose of this document is to provide a clear, comprehensive, and transparent description of MKD-GOV-CSIRT, in accordance with the requirements set forth in RFC 2350. The document presents the organizational structure and composition of the team, defines the official communication and contact channels, and outlines the responsibilities, authorities, and services provided by MKD-GOV-CSIRT.

Additionally, the document provides guidance and information on the procedures for reporting and handling cybersecurity incidents affecting the network and information systems under the responsibility of MKD-GOV-CSIRT, with the aim of enhancing coordination, efficiency, and cooperation with relevant stakeholders.

Ministry of Digital Transformation of the Republic of North Macedonia
St. „Phillip II of Macedon" no. 11, Skopje
Republic of North Macedonia
+389 2 320 0999
www.mdt.gov.mk

1.3. Scope

The scope of this document covers the network and information systems of public sector institutions of the Republic of North Macedonia, including the systems of the Government, ministries, state administration bodies and organizations, as well as the systems of local self-government units, the municipalities within the City of Skopje, and the City of Skopje.

1.4. References

RFC2350

2. Document Information

2.1. Date of Last Update

This version of the document remains valid until the publication of a new document with a subsequent version number.

2.3. Location of This Document

The current valid version is continuously available on the official website of the Ministry of Digital Transformation.

2.4. Document Authentication

This document is signed with the PGP key of MKD-GOV-CSIRT.

The signature is available on the official website of the Ministry of Digital Transformation / MKD-GOV-CSIRT.

3. Contact Information

3.1. Team Name

Full Name: Computer Security Incident Response Team for Executive Authorities

Short Name: MKD-GOV-CSIRT

Ministry of Digital Transformation of the Republic of North Macedonia
St. „Phillip II of Macedon" no. 11, Skopje
Republic of North Macedonia
+389 2 320 0999
www.mdt.gov.mk

3.2. Address

Ministry of Digital Transformation

St. Philip Vtori Makedonski no. 11

1000 Skopje, Republic of North Macedonia

3.3. Time Zone

CET / CEST

Central European Time / Central European Summer Time

3.4. Telephone Number

Working Hours: + 3240 900

Emergency Number: +38980021111

3.5. Other Telecommunications

Website: https://mdt.gov.mk/mk-MK/mkd-gov-csirt

3.6. Email Addresses

cyber.security@csirt.gov.mk

3.7. Public Key and Encryption Information

The email address cyber.security@csirt.gov.mk used by MKD-GOV-CSIRT shares the same PGP-ключ, as documented below:

- **Key ID:** 0F304D6A8BD0791B
- **Key Type:** RSA 4096
- **Key Fingerprint:** 2D22D1F0983C08BC5DCD0DEB0F304D6A8BD0791B

Public key:

The public key and its signatures can be found on the standard major public key servers, as well as on the MDT website https://mdt.gov.mk/mk-MK/mkd-gov-csirt. This key

is used to sign all communications from MKD-GOV-CSIRT. It is also used for any confidential communication with MKD-GOV-CSIRT (incident reports, alerts).

3.8. MKD-GOV-CSIRT Team Members

MKD-GOV-CSIRT is composed of cybersecurity professionals employed by the Ministry of Digital Transformation. For security reasons, the full list of team members is not publicly available. During official communication related to a cybersecurity incident, team members identify themselves to the reporting party by their full name and official position.

3.9. Other Information

General information about MKD-GOV-CSIRT, as well as links or references to other recommended information security resources, can be found on the public website of MDT-MKD-GOV-CSIRT https://mdt.gov.mk/mk-MK/mkd-gov-csirt.

3.10. User Contact Points

MKD-GOV-CSIRT Working Days/Hours:

The preferred method of contacting the MKD-GOV-CSIRT team is by sending an email to the address cyber.security@csirt.gov.mk, which is monitored by an on-duty staff member 24/7.

Contact Phone: + 3240 900

Emergencies: Can be reported 24/7 by phone at +38980021111

Working Hours: 08:00 to 16:00, Monday to Friday (excluding public holidays)

4. Charter

4.1. Mission Statement of MKD-GOV-CSIRT

The mission of MKD-GOV-CSIRT is to build and maintain a secure, stable, and resilient cyber environment within the Government and the state administration bodies, through an integrated approach to managing cyber risks and incidents.

MKD-GOV-CSIRT fulfills its mission through:

- Prevention and management of computer security incidents;
- Coordination and information exchange on cyber threats with the national CSIRT and other relevant institutions;
- Supporting constituents in the identification, analysis, and resolution of cyber incidents;
- Providing strategic and operational guidance for the implementation of cybersecurity measures;
- Promoting awareness of cyber threats and the use of security tools and standards.

The mission of MKD-GOV-CSIRT is to provide a trusted, integrated, and effective national mechanism for responding to cyber incidents, aiming to protect the critical systems of the Government and the public sector, as well as to support national cybersecurity.

4.2. Constituents of MKD-GOV-CSIRT include:

The constituents of MKD-GOV-CSIRT are the institutions whose network and information systems fall under the team's responsibility, including:

- The Government of the Republic of North Macedonia;
- Ministries;
- State administrative bodies and organizations;
- Local self-government units, including the municipalities within the City of Skopje and the City of Skopje.

Ministry of Digital Transformation of the Republic of North Macedonia
St. „Phillip II of Macedon" no. 11, Skopje
Republic of North Macedonia
+389 2 320 0999
www.mdt.gov.mk

4.3. Sponsorship/Support and Affiliation

MKD-GOV-CSIRT was established and sponsored by the Ministry of Digital Transformation as part of the Government of the Republic of North Macedonia. The team collaborates and exchanges information with:

- MKD-CIRT, the National Computer Incident Response Center, for coordination and joint incident handling;
- Domestic CSIRT/CERT teams;
- International organizations and networks for managing cyber incidents and crises, including EU-CyCLONe;

4.4. Authority

In accordance with Article 12 of the Law on the Security of Network and Information Systems ("Official Gazette of the Republic of North Macedonia" No. 135/2025), MKD-GOV-CSIRT is the Team for Computer Incident Response for executive authorities, operating as an organizational unit within the Ministry of Digital Transformation.

Within its scope of competence, MKD-GOV-CSIRT:

- carries out prevention, early detection, analysis, and coordinated response to cybersecurity threats and incidents affecting entities under its jurisdiction;
- prepares plans, protocols, and technical guidelines for managing cyber risk management, significant incidents, and cyber crises;
- issues warnings, notifications, recommendations, and provides expert support to executive authorities and other entities as defined by law;
- maintains registers and records of incidents, critical sectors, and entities in accordance with legal provisions;
- cooperates and exchanges information with the National Computer Incident Response Center (MKD-CIRT), competent state authorities, as well as domestic and international organizations and networks;
- performs oversight of essential and important entities within its legal mandate and proposes or imposes measures in accordance with the law;
- organizes and conducts training sessions, exercises, and activities aimed at raising awareness and strengthening cybersecurity capacities;
- prepares annual reports and other strategic and operational documents in the field of cybersecurity;
- performs other tasks as prescribed by law.

Ministry of Digital Transformation of the Republic of North Macedonia
St. „Phillip II of Macedon" no. 11, Skopje
Republic of North Macedonia
+389 2 320 0999
www.mdt.gov.mk

5. Policies

5.1. Types of Incidents and Support Levels

MKD-GOV-CSIRT, as the Computer Security Incident Response Team for executive government bodies, handles cybersecurity incidents and threats affecting the network and information systems of entities under its jurisdiction, in accordance with legal definitions and obligations.

Incidents are classified based on their impact on the availability, confidentiality, integrity, or functioning of systems, including, among others, significant cybersecurity incidents and other incidents that may cause service disruption, financial losses, or harm to users.

The level of support provided by MKD-GOV-CSIRT varies depending on the severity, scope, and potential impact of the incident, as well as the available resources, with priority given to incidents that significantly affect critical systems of the Government and the public sector.

5.2. Collaboration, Interaction, and Information Disclosure

MKD-GOV-CSIRT highly values operational collaboration and information sharing with:

- The National CIRT (MKD-CIRT);
- Other governmental and public institutions;
- International CSIRT and CERT networks;
- Constituents and other organizations that can contribute to security.

All received information is treated as confidential. Shared information is disclosed only to authorized parties and is classified according to the Traffic Light Protocol (TLP). MKD-GOV-CSIRT protects sensitive information in accordance with the legal regulations of the Republic of North Macedonia.

5.3. Communication and Authentication

The preferred method of communication with MKD-GOV-CSIRT is via email. If this is not possible or advisable for security reasons (for example, for sensitive data), MKD-GOV-CSIRT is available during working hours by telephone. Outside of working hours, an on-call phone number is available, with accessibility applied on a best-effort basis.

Ministry of Digital Transformation of the Republic of North Macedonia
St. „Phillip II of Macedon" no. 11, Skopje
Republic of North Macedonia
+389 2 320 0999
www.mdt.gov.mk

Telephone communication can be used as a sufficiently secure method for exchanging unclassified or low-sensitivity information, even without encryption. Unencrypted email messages are not considered sufficiently secure for confidential data but are acceptable for unclassified information.

When trust needs to be established, for example before transmitting information to MKD-GOV-CSIRT or before disclosing confidential data, secure authentication of the sender's identity is required.

Communication security is ensured through methods such as PGP or other pre-agreed mechanisms, depending on the sensitivity level of the information.

When sending sensitive data via email or network transfers, the data must be encrypted using MKD-GOV-CSIRT keys. All data communications, including those initiated by MKD-GOV-CSIRT, are digitally signed using the team's PGP keys or the digital signature keys of an authorized employee.

The use of encryption and digital signatures is recommended when sending information to MKD-GOV-CSIRT, especially for sensitive or confidential data.

When submitting an incident report, it is necessary to provide:

- A note on the urgency of the incident;
- The need for feedback;
- The incident report form.

6. Services

MKD-GOV-CSIRT is authorized to manage and respond to all types of computer security incidents that occur or threaten to occur in the networks, systems, and services of public sector institutions in the Republic of North Macedonia, including the systems of the Government, ministries, state administration bodies, and local self-government units.

MKD-GOV-CSIRT provides support to its constituents through a range of reactive and proactive cybersecurity services, including:

Information Security Event Management, which includes:

- Monitoring and detection,
- Event analysis.

Information Security Incident Management, which includes:

- Information security incident report acceptance,
- Information security incident analysis,
- Information security incident coordination.

MKD-GOV-CSIRT coordinates incident management activities in accordance with the applicable Law on the Security of Network and Information Systems and cooperates with the National CIRT (MKD-CIRT) for information exchange and coordination during high-impact or high-criticality incidents.

7. Incident Report Form

Incident reporting within MKD-GOV-CSIRT can be done in one of the following two ways:

1. Anonymous Method – Reporting an incident using the MKD-GOV-CSIRT web form. Incidents reported this way are submitted anonymously. Data submitted through the web form is encrypted before transmission using the MKD-GOV-CSIRT public key, ensuring confidentiality.
2. Standard Method – Reporting an incident using the Incident Report Form according to the Incident Reporting Guidelines, available on the official MKD-GOV-CSIRT website.

Ministry of Digital Transformation of the Republic of North Macedonia
St. „Phillip II of Macedon" no. 11, Skopje
Republic of North Macedonia
+389 2 320 0999
www.mdt.gov.mk