GUIDELINE FOR REPORTING INCIDENTS BY CONSTITUENTS

I. GENERAL PROVISIONS

Article 1

This Guideline regulates the manner of reporting cybersecurity incidents by the constituents of MKD-GOV-CSIRT, the content of the report, reporting deadlines, as well as the handling of reported incidents. It also regulates the competencies, role, and services provided by the Computer Incident Response Team MKD-GOV-CSIRT.

Article 2

Constituents of MKD-GOV-CSIRT are the Government of the Republic of North Macedonia, ministries, independent state administration bodies, administrative bodies within ministries, administrative organizations, municipalities, municipalities within the City of Skopje, and the City of Skopje. Constituents are obliged to act in accordance with the provisions of this Rulebook when reporting and managing cybersecurity incidents.

Article 3

The purpose of this guideline is to assist constituents in reporting cybersecurity incidents to MKD-GOV-CSIRT within the required timeframe.

II. DEFINITIONS

Article 4

Security of network and information systems is the ability of network and information systems to resist, with a certain level of confidence, any action that compromises the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data or the related services offered by or accessible through those systems.

Article 5

A significant cyber threat is a cyber threat which, based on its technical characteristics, can be assumed to have a serious impact on network and information systems of an entity or on the users of that entity's services by causing substantial material or non-material damage.

Article 6

A significant cybersecurity incident is an incident that has caused or may cause serious disruption in the functioning of services or financial losses for the relevant essential or important entity, and may affect other natural or legal persons by causing significant material or non-material damage.

Article 7

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

An incident is any event that compromises the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data or services offered by or accessible through network and information systems.

Article 8

A Cybersecurity Officer is a person mandatorily engaged by essential entities, possessing appropriate professional competencies, responsible for implementing cybersecurity measures defined by the Law on Security of Network and Information Systems ("Official Gazette of the Republic of North Macedonia" No. 135 of 04.07.2025), and who directly communicates and cooperates with the competent authority and the competent Computer Incident Response Team for consistent implementation of the law.

Article 9

Cybersecurity is a system of activities and measures necessary to protect network and information systems, users of such systems, and other persons affected by threats via computer networks.

Article 10

A cyber threat is any potential circumstance, event, or activity that may damage, disrupt, or otherwise negatively affect network and information systems, their users, or other persons.

Article 11

A Computer Incident Response Team (CSIRT) is a body responsible for handling incidents in accordance with a prescribed procedure.

Article 12

Essential entities from the perspective of the security of network and information systems are large entities operating in the sectors of energy, transport, banking, financial market infrastructures, healthcare, digital infrastructure, ICT service management, drinking water supply and distribution, wastewater, postal and courier services, waste management, manufacture, production and distribution of chemicals, production, processing and distribution of food, manufacturing, digital service providers and research, providers of qualified trust services, top-level domain name registries (the .mk and .мкд domains) or DNS service providers, regardless of their size, operators and/or providers of public electronic communications networks and/or publicly available electronic communications services considered medium-sized and large entities, public sector institutions, the Assembly, independent state bodies and regulatory authorities established by and accountable to the Assembly, the Government, ministries, independent bodies of state administration, state administration bodies, administrative bodies within ministries, administrative organizations, courts and municipalities, the municipalities within the City of Skopje and the City of Skopje, entities which, regardless of their size, belong to the group of entities providing trust services and the entity managing the Single Register of Top-Level Domains (the .mk and .мкд domains), entities identified as owners/operators of critical infrastructure, entities designated as essential entities in accordance with national legislation, and other entities which, pursuant to law or based on a risk assessment, are determined to be essential entities.

Article 13

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

Important entities, from the perspective of the security of network and information systems, are all entities from the detailed list of sectors of high criticality and from the detailed list of sectors and types of entities of high criticality that do not fall within the category of essential entities, as well as other entities which, pursuant to law or based on a conducted risk assessment, are determined to be important entities.

III. COMPETENCIES AND SERVICES OF MKD-GOV-CSIRT

Article 14

MKD-GOV-CSIRT is responsible for managing and responding to all types of computer security incidents occurring or potentially occurring in the networks, information systems, and services of constituents. The team monitors security threats, analyzes incidents, coordinates response activities, and provides expert support.

Article 15

MKD-GOV-CSIRT provides support to constituents through reactive and proactive cybersecurity services. The team continuously monitors and detects security events, analyzes them, and coordinates incident management activities. It receives incident reports, performs analysis, and coordinates resolution activities in cooperation with affected constituents.

Article 16

MKD-GOV-CSIRT coordinates incident management activities in accordance with applicable legislation and cooperates with the national team MKD-CIRT for information exchange and coordination in high-severity incidents.

IV. INCIDENT REPORTING AND RESPONSE

Article 17

Constituents are obliged to immediately, and no later than three (3) hours from becoming aware of the incident and/or cyber threat, notify MKD-GOV-CSIRT of any significant cybersecurity incident and/or significant cyber threat affecting their services, and provide all necessary information to determine any cross-border impact.
Timely reporting is essential for effective incident management and mitigation.

Article 18

Where possible, constituents must immediately, and no later than the next working day after becoming aware of a cyber threat, inform users of their services who may be affected by a serious cyber threat about measures or legal remedies they can take, and, if necessary, about the threat itself.

Article 19

Within 24 hours of becoming aware of a significant cybersecurity incident, constituents must submit an early warning to MKD-GOV-CSIRT, indicating, where appropriate, whether the incident is suspected to be caused by unlawful or malicious activity or may have cross-border impact.

Article 20

Within 72 hours, constituents must submit an incident notification including:

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

- an initial assessment of the incident,
- its severity and impact,
- indicators of compromise, if available.

Article 21

Within one month after submitting the notification of the significant cybersecurity incident, constituents are required to submit a final report to MKD-GOV-CSIRT, including the following:

- detailed description of the incident,
- type of threat or root cause,
- mitigation measures applied,
- cross-border impact, if applicable.

Article 22

If the incident is ongoing, a progress report must be submitted, followed by a final report within one month after resolution.

Article 23

MKD-GOV-CSIRT shall, within 24 hours of receiving the early warning, provide the constituent with a response, including initial feedback on the significant cybersecurity incident, and, upon the constituent's request, provide guidance or operational advice regarding the implementation of possible mitigation measures, as well as additional technical support.

Article 24

If MKD-GOV-CSIRT is not the initial recipient, guidance is provided by the competent authority in cooperation with MKD-GOV-CSIRT.

Article 25

MKD-GOV-CSIRT provides additional technical support if requested by the constituent.

Article 26

If there is suspicion of a criminal offense, MKD-GOV-CSIRT will instruct reporting to competent authorities.

Article 27

If informing the public is necessary to prevent or address an ongoing significant cybersecurity incident, or if the disclosure of the significant incident is otherwise in the public interest, the Ministry of Digital Transformation may, after consulting with the affected essential or important entity, inform the public about the significant cybersecurity incident or request the respective entity to do so.

Article 28

Any personal data contained in reports on significant cybersecurity incidents shall be limited to what is strictly necessary for the description and resolution of the incident.

Article 29

Information is classified according to TLP (Clear, Green, Amber, Amber Strict, Red), with protection levels defined as Public, Confidential, or Strictly Confidential.

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

Article 30

The report may be submitted through:

- the Ministry's portal referred to in Article 15, paragraph (5) of the Law (primary channel, mandatory when available), using the official Incident Reporting Form;
- electronic mail (electronically signed and encrypted);
- telephone communication in emergency cases.

Article 31

Upon receipt, MKD-GOV-CSIRT issues confirmation including an incident reference number.

Article 32

Upon receipt of a report from a constituent, MKD-GOV-CSIRT initiates incident management in accordance with its legal competencies. The team carries out identification, analysis, and coordination of the response, and, where necessary, provides technical support to the constituent, with the aim of effectively managing cybersecurity threats and incidents, in accordance with the Law on Network and Information Systems Security.

V. VOLUNTARY NOTIFICATIONS

Article 33

Constituents may, on a voluntary basis, submit notifications to MKD-GOV-CSIRT regarding cybersecurity incidents, cyber threats, and near-misses that are not significant, in accordance with Article 38 of the Law.

Entities that are not within the scope of this guidance may also submit voluntary notifications concerning significant or non-significant incidents, cyber threats, and near-misses.

MKD-GOV-CSIRT gives priority to mandatory notifications over voluntary ones. In accordance with Article 38, paragraph (5) of the Law, voluntary notification does not create any additional obligations for the notifier.

MKD-GOV-CSIRT forwards voluntary notifications to the Ministry as the single point of contact.

VI. FINAL PROVISIONS

Article 32

This guideline is reviewed and updated as needed, at least annually.

Article 33

This guideline enters into force on the day of signing by the responsible person in the Ministry of Digital Transformation.

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