Republic of North Macedonia

Ministry of Digital Transformation

METHODOLOGY FOR THE CLOSE-UP CRITERIA, AS WELL AS THE THRESHOLD FOR DETERMINING ORDINARY AND SIGNIFICANT CYBER SECURITY INCIDENTS

GENERAL PROVISIONS

Purpose
Article 1

This Methodology prescribes the more detailed criteria, as well as the threshold for determining ordinary and significant cybersecurity incidents for the Government, ministries, independent state administration bodies, state administration bodies including ministries, administrative organizations, municipalities, municipalities in the city of Skopje and the city of Skopje.

Article 2

The Methodology is intended for rapid identification and classification of cybersecurity incidents, decision-making on escalation, prioritization in the recovery phase from cybersecurity incidents, as well as consistent reporting and analysis of the cybersecurity incidents that have occurred.

CLASSIFICATION OF CYBER SECURITY INCIDENTS

Classification
Article 3

Cyber security incidents are classified into the following categories:

Category 1	Compromise incidents
Category 2	Service disruption incidents
Category 3	Threat or vulnerability incidents

Compromise incidents
Article 4

Compromise incidents are events in which there is unauthorized access, compromise of systems, networks or applications and/or violation of the confidentiality and/or integrity of data.

Basic features	• unauthorized access • compromise of systems, networks or applications

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

	• violation of the confidentiality • violation of integrity
Scope	• malicious software (ransomware, spyware, backdoor), • unauthorized access or takeover of user accounts, • data leakage or theft, • exploitation of vulnerabilities, • insider incidents, • supply chain compromises

Service disruption incidents
Article 5

Service disruption incidents are events that lead to partial or complete interruption of ICT services, degradation of performance, or incapacitation of systems or infrastructure:

Basic features	• partial or complete interruption of ICT services, • performance degradation, • disabling systems or infrastructure.
Scope	• DoS/DDoS attacks, • ransomware blocking systems, • sabotage of ICT resources, • disruptions caused by a security event.

Incidents with threat or weakness
Article 6

Threat or vulnerability incidents are events that did not result in a direct compromise or disruption but pose a real risk to security:

Basic features	**Potential security risk without actual damage**
Scope	• phishing and other forms of social engineering, • identified technical vulnerabilities, • incorrect configurations, • violations of security policies, • physical security weaknesses

ASSESSMENT CRITERIA

Specific criteria for assessing cyber security incidents
Article 7

The assessment of cybersecurity is carried out based on the following closer criteria, regardless of their classification and whether the incident has:

Criteria	**Level / Description**
1. Impact on confidentiality, integrity and availability (CIA)	• No impact, • Limited/local impact, • Significant impact.

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

	• Serious or complete disruption
2. Scope and prevalence	• Single system or user, • Multiple systems, • Multiple organizational units • Multiple institutions/cross-border
3. Intentionality and complexity	• Random/unintentional event, • Simple, undirected attack, • Targeted attack • Coordinated or advanced attack.
4. Duration and recovery	• short-term (< 1 hour), • medium (1–4 hours), • long-term (4-24 hours), • need for external or specialized support (>24 hours).
5. Legal, regulatory and reputational impact	• no obligation to report, • Internal reporting, • National obligation to report to MKD GOV-CSIRT • International impact/serious reputational risk.

THRESHOLD FOR DETERMINING SIGNIFICANCE

Article 8

According to the significance, cyber security incidents can be divided into 2 (two) types, as follows:

Type of incident	Full criteria
Ordinary cyber security incidents	• the impact is low or limited, • a small number of systems or users are affected, • there is no leakage of sensitive data, • there is no significant disruption of services, • can be resolved with standard operating procedures, • there is no legal obligation for external reporting.
Significant cybersecurity incidents	• serious breach of confidentiality, integrity or availability, • compromise or leakage of sensitive, personal or classified data, • interruption or significant disruption of public or critical services, • multiple systems or institutions are affected, • there is a suspicion of a coordinated or advanced attack, • escalation to a national MKD-GOV-CSIRT is required, • there is a legal or international obligation to report,

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

	• the incident has the potential for widespread recurrence or systemic risk.

FINAL PROVISIONS

Entry into force

Article 9

This Methodology shall enter into force on the day of its publication in the "Official Gazette of the Republic of North Macedonia"

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