Republic of North Macedonia

Ministry of Digital Transformation

POLICY ON INFORMATION DISCLOSURE (TRAFFIC LIGHT PROTOCOL-TLP)

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

Republic of North Macedonia

Ministry of Digital Transformation

CONTENT:

1. Introduction 2
1.1 Purpose 3
1.2. Scope 3
1.3. References 3
2. Definitions 4
2.1. Information Exchange 4
2.2. Anonymization 4
3. Data Management Responsibility 4
4. Information Disclosure 4
4.1. Information Protection 4
4.2. Collaboration with Other Parties 5
4.3. Communication Security: 5
4.4. Personal Data Protection and Legal Aspects 5
4.5. Anonymization 5
4.6. Use of TLP for Information Sharing 6
4.6.1. General Principles 6
4.6.2. Standard TLP Classification Level 6
Annex 1 – Use of TLP (Traffic Light Protocol) for Information Sharing 7
Annex 2 – Information Exchange 8

1. Introduction

The handling of sensitive information is a core aspect of the daily operations of the Government Computer Security Incident Response Team – MKD-GOV-CSIRT, which functions under the Ministry of

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

Digital Transformation. Sensitive information may be submitted to MKD-GOV-CSIRT through cybersecurity incident reports from state administration bodies, institutions, as well as other relevant stakeholders involved in the management of cybersecurity incidents and threats.

Maintaining trust in MKD-GOV-CSIRT's capability to appropriately protect, handle, and share sensitive information in a controlled manner is crucial for the effective fulfillment of its statutory responsibilities. Accordingly, the rules for information disclosure and sharing outlined in this document are intended to provide clear guidance and principles to ensure a high level of confidentiality, integrity, and trust in MKD-GOV-CSIRT's operations.

1.1 Purpose

The purpose of this policy is to define and describe the principles, rules, and limitations that MKD-GOV-CSIRT applies when disclosing, publishing, and sharing information within the scope of its operations.

This policy, together with the MKD-GOV-CSIRT Information Classification Policy, forms an integral part of the information management framework and aims to ensure the confidentiality, integrity, and availability of the data handled by MKD-GOV-CSIRT.

1.2. Scope

This policy applies to all information and information assets that are created, received, processed, managed, stored, transmitted, or otherwise recorded by MKD-GOV-CSIRT, regardless of their form or medium.

The policy is mandatory for all employees, engaged personnel, and other entities who, based on law, authorization, contract, or established collaboration, have access to information handled by MKD-GOV-CSIRT.

1.3. References

- **Laws**
  - Law on Security of Network and Information Systems
  - Law on Personal Data Protection
  - Law on Electronic Communications
  - Law on Classified Information

- **Internal Policies and Templates of MKD-GOV-CSIRT**
  - Information Classification Policy
  - Template: Authorization to Disclose Information
  - Template: Non-Disclosure Agreement (NDA)

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

- **International Guidelines and Standards for TLP 2.0**
  - FIRST.org – Traffic Light Protocol (TLP)
  - CISA – TLP 2.0 User Guide
  - CERT-EU Blog – TLP Version 2 Primer

2. Definitions

2.1. Information Exchange

Information exchange is the transfer or sharing of information between MKD-GOV-CSIRT, its constituents, and other relevant parties. This may occur:

- **In person**, during meetings of CSIRT teams or with MKD-GOV-CSIRT constituents.
- **At meetings** involving cybersecurity experts.
- **Electronically**, via email, secure platforms, or telephone calls.

2.2. Anonymization

Anonymization is the process of removing or replacing identifying information about individuals or organizations in order to protect privacy and maintain the confidentiality of data when it is shared.

3. Data Management Responsibility

All members of **MKD-GOV-CSIRT** are obligated to protect the confidentiality of the data they handle, regardless of the form or medium in which the data is recorded or transmitted, in accordance with the operational procedures of MKD-GOV-CSIRT.

MKD-GOV-CSIRT is responsible for implementing appropriate procedural, physical, and technical controls for the access, use, transmission, or storage of data owned or used by MKD-GOV-CSIRT, in accordance with this policy.

To prevent any leakage of sensitive information, members of MKD-GOV-CSIRT shall disclose information only when necessary and in accordance with the rules defined in this policy.

4. Information Disclosure

4.1. Information Protection

When exchanging information, MKD-GOV-CSIRT applies the “need-to-know” principle:

- Information that is not public must not be shared publicly and should be disclosed only to those entities that need to know it.

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

- Disclosure and sharing of information must be conducted in accordance with its original level of confidentiality.
- MKD-GOV-CSIRT respects the classification assigned to the information by the source that provided it, in accordance with internal operational procedures.
- Disclosure and publication of sensitive information occur only when necessary for incident resolution. Principles for data anonymization are outlined in Section 4.4.

4.2. Collaboration with Other Parties

MKD-GOV-CSIRT frequently collaborates with other CSIRT teams, relevant stakeholders, vendors, suppliers, and governmental authorities.

The disclosure of information to these groups is conducted on a case-by-case basis and is proportional to the risk associated with sharing the information. Before disclosing information, MKD-GOV-CSIRT may require the signing of a Non-Disclosure Agreement (NDA).

The integrity and trustworthiness of partners are verified prior to the exchange of confidential information.

4.3. Communication Security:

Whenever information is made available to others:

- It must be signed to ensure non-repudiation.
- It must be encrypted to protect confidentiality, whenever required in accordance with this policy.

4.4. Personal Data Protection and Legal Aspects

MKD-GOV-CSIRT provides requested information to state authorities, public institutions, or authorized third parties only when there is a legal obligation to do so. This means that every disclosure is carried out in compliance with all relevant legal requirements, for example, through the delivery of a court order or other official act, in order to ensure the legitimacy and legal protection of the process.

Every case of processing or transfer of personal data, in terms of form and content, will be conducted in accordance with the Law on Personal Data Protection, the Law on Classified Information, the Law on Electronic Communications, and other applicable regulations in the Republic of North Macedonia, taking into account the policies and classification decisions of NATO and the European Union.

4.5. Anonymization

According to the definition in Section 2.2, sensitive information will always be anonymized before being shared with a third party. This means that personal data or other information that could be used to identify subjects or targets of a cyber attack will not be exchanged, unless explicit written consent is obtained from the data owner or the data has been properly anonymized.

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

Information exchange with third parties occurs only when necessary for incident resolution.

In cases where anonymization is not practical or would be counterproductive for handling the incident, MKD-GOV-CSIRT reserves the right to share non-anonymized information only with groups or third parties with whom a trusted relationship has been established.

All such exchanges are carried out in accordance with the applicable laws of the Republic of North Macedonia, and with the explicit written approval of the owner of the information being shared (using the Template – Authorization to Disclose Information).

4.6. Use of TLP for Information Sharing

4.6.1. General Principles

To protect the information it processes and shares, MKD-GOV-CSIRT will apply its Information Classification Policy together with the Traffic Light Protocol (TLP) as a framework for controlled sharing.

When exchanging information, MKD-GOV-CSIRT will label the information with the appropriate TLP designation only with parties that have accepted the use of TLP. If the party with whom the information is being exchanged does not implement the TLP protocol, MKD-GOV-CSIRT will initiate a verification and alignment of the confidentiality levels used by both parties before sharing the information.

The rules and general principles of TLP are provided in the Annex – Use of TLP (Traffic Light Protocol) for Information Sharing and are part of this policy.

Any communication or exchange of information above TLP: GREEN, including emails or documents, must be labeled with the designation "[TLP: Color]", where Color can be RED, AMBER+STRICT, AMBER, GREEN, or CLEAR. A similar label or stamp must be clearly visible at the beginning of the message or on the cover/header of any document sent or published by MKD-GOV-CSIRT.

If the communication is conducted verbally, for example via a telephone call or video conference, the appropriate TLP level must be clearly stated at the beginning of the conversation, before any information is disclosed.

4.6.2. Standard TLP Classification Level

As an initial level, MKD-GOV-CSIRT may use TLP:AMBER, but the final classification of the information is determined based on a risk assessment, the context of the incident, and the guidelines of FIRST TLP 2.0.

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

Republic of North Macedonia

Ministry of Digital Transformation

Annex 1 – Use of TLP (Traffic Light Protocol) for Information Sharing

All information exchanged by MKD-GOV-CSIRT must be labeled with the appropriate TLP designation according to the following table. If the information being exchanged has not been previously labeled by the source, MKD-GOV-CSIRT will automatically assign TLP:AMBER.

LABEL	USAGE DESCRIPTION
TLP RED	INFORMATION NOT TO BE DISCLOSED – restricted only to representatives of the participants in the information exchange. Representatives must not share the information outside of the participants in the exchange. For information labeled TLP RED, discussion may occur only during the exchange itself, when all participants in the exchange agree to it. Individuals or parties who are not participants in the TLP RED information exchange MUST NOT be present during the exchange or discussion of the information.
TLP AMBER	INFORMATION WITH LIMITED DISCLOSURE – intended only for members of the information exchange: members of organizations or constituents (direct employees, consultants, or other engaged personnel) who meet the "NEED-TO-KNOW" requirement in order to act on the information.
TLP AMBER+STRICT	INFORMATION WITH LIMITED DISCLOSURE – intended only for members of the organization or constituent who need to know it in order to act on the information. It may be shared only within the organization and only with those who meet the "need-to-know" principle, to protect the organization and prevent further harm.
TLP GREEN	INFORMATION MAY BE SHARED WITH OTHER ORGANIZATIONS – during information exchange with individuals and cybersecurity experts, but it must not be published publicly or posted on a public website.
TLP CLEAR	PUBLIC INFORMATION – there are no restrictions on its dissemination, publication, posting on public websites, or broadcast. Any member of the information exchange may publish the information while respecting intellectual property rights.

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

Annex 2 – Information Exchange

Level / Contact	Information Exchanged	Responsible Person	Storage / Technical Processing	Dissemination Level
Internal – Organization	Team data, SOPs, shift planning, internal contacts	Head of Cyber Security Sector + Head of Department for Preparation and Coordination of Cyber Security Policies	RTIR / SIEM / MIOShare	Internal
National – Other Institutions and Constituents	Incident notifications, TTPs, reports, alerts, affected systems	Advisor for Network and Information Systems Security at the Ministry + Advisor for Network and Information Systems Security in other public sector institutions	RTIR / SIEM / MIOShare	Restricted (at the level of constituents and partner institutions)
International – Other CSIRTs (FIRST, regional CSIRTs), international partners	IOCs, threat reports, TTPs, alerts, meeting invitations, notifications	Junior Associate for International Communications + Advisor for Preparation of Cybersecurity Regulations + Advisor for Network and Information Systems Security at the Ministry	RTIR / MIOShare / secure email	Restricted / confidential for international partners

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