Republic of North Macedonia

Ministry of Digital Transformation

CLASSIFIED INFORMATION POLICY

1. Introduction

The effective functioning of public institutions depends on the continuous processing, exchange, and storage of large volumes of information, a portion of which is sensitive or classified. Unauthorized access, disclosure, or misuse of such information may result in serious institutional, legal, and national security consequences.

Pursuant to the Constitution of the Republic of North Macedonia and the Law on Classified Information, the Ministry of Digital Transformation establishes this Classified Information Policy.

This policy provides a strategic and governance framework for the classification, management, protection, and controlled sharing of information across its entire lifecycle.

The policy is aligned with national legislation and internationally recognized information security standards and best practices, including:

- ISO/IEC 27001 and ISO/IEC 27002
- FIRST Traffic Light Protocol (TLP) guidance
- SIM3 Security Operations Maturity Model

Its purpose is to ensure regulatory compliance and to establish a consistent, risk-based, and standardized approach to the protection of classified and sensitive information.

2. Purpose

The purpose of this policy is to establish clear, structured, and legally compliant rules for the classification, labeling, use, sharing, and protection of all information handled by the Ministry of Digital Transformation.

This policy aims to:

- ensure the protection of classified and sensitive information;
- reduce the risk of unauthorized access, disclosure, loss, or misuse of information;
- ensure compliance with the Law on Classified Information and related regulations;
- establish clear access control based on the **need-to-know** principle;
- enable secure and controlled information sharing through the Traffic Light Protocol (TLP);
- provide a consistent lifecycle-based approach to information management;
- strengthen awareness and accountability of employees and partners regarding information protection.

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. Scope

This Policy applies to all information related to the constituents of MKD-GOV-CSIRT that is created, received, processed, stored, or shared by the Ministry of Digital Transformation, regardless of its form, format, or medium.
The policy covers the following categories:

Information

- All paper-based documents
- Electronic documents, databases, and information processing systems
- Email, official correspondence, and communications
- Audio, video, and multimedia records
- Working materials, reports, analyses, and official notes

Persons

- Employees of the Ministry of Digital Transformation
- Contractors and collaborators
- Suppliers and external partners
- Third parties granted access to information

Processes

- Creation, receipt, and processing of information
- Storage and retention of information
- Sharing and transfer of information
- Archiving and destruction
- Access control and handling of information in accordance with classification levels and TLP markings.

4. Definitions

This section defines the key terms and concepts used in the Information Classification Policy to ensure a consistent and shared understanding of the measures and procedures for classifying, handling, and protecting information.

1. Information

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 refers to knowledge that can be communicated in any form, including records, data, documents, or communications created, received, stored, or shared by the Ministry of Digital Transformation, regardless of format (paper, electronic, or digital).

2. Information of Interest to the Republic of North Macedonia

Information of interest to the Republic of North Macedonia is information categorized according to its level of sensitivity and protection requirements, with access restricted to authorized persons.

3. Classified Information

Classified information is information that:

- relates to public security, defense, foreign affairs, or intelligence and security activities;
- falls within the scope of work of state or local authorities or state-established legal entities;
- must be protected from unauthorized access and is marked with an appropriate classification level.

4. Need-to-Know Principle

The **need-to-know** principle ensures that access to classified information is granted only to individuals who:

- hold the appropriate security clearance; and
- have a legitimate operational requirement to access the information in order to perform their duties or responsibilities.

5. Handling of Classified Information

Handling classified information refers to the full lifecycle management of information, including:

- creation and receipt;
- registration and marking;
- use and processing;
- transfer and sharing;
- archiving;
- reclassification or declassification;
- secure destruction.

All activities must be performed in accordance with classification rules and the application of TLP markings.

5. Traffic Light Protocol (TLP)

In addition to the national classification system, the Ministry of Digital Transformation applies the Traffic Light Protocol (TLP) as an operational mechanism for the controlled sharing of sensitive information.

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

TLP provides a practical framework for:

- restricting the distribution of information;
- enabling controlled information sharing with partners;
- reducing the risk of information compromise;
- supporting cybersecurity collaboration.

The application and handling of TLP labels shall be performed in accordance with the MDT Policy on Information Disclosure (TLP), developed in alignment with FIRST TLP standards.

6. Classification Levels

The Ministry of Digital Transformation applies the national information classification system. The classification level is determined by the information creator or an authorized person based on the content and the potential impact of unauthorized disclosure.

Information is classified into the following levels:

STATE SECRET
- Unauthorized disclosure would cause irreparable damage to the permanent interests of the Republic of North Macedonia.

TOP SECRET
- Unauthorized disclosure would cause exceptionally serious damage to the vital interests of the state.

CONFIDENTIAL
- Unauthorized disclosure would cause serious damage to the important interests of the state.

INTERNAL
- Unauthorized disclosure would cause harm to the operations of institutions and legal entities relevant to public security, defense, foreign affairs, and intelligence and security activities.

Administrative Security

Administrative security establishes the governance processes for the classification, registration, and lifecycle management of classified information.

a. Classification and Marking

All information must be classified immediately upon creation or receipt. Classification is performed by the information creator or an authorized person.

All classified information must:

- be clearly marked with the appropriate classification level;

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

- include a TLP classification;
- be properly labeled in both electronic and physical formats.

b. Receipt and Registration of Classified Information

All received classified information must be recorded in an appropriate registry to ensure traceability and accountability.

The registry must include:

- date of receipt;
- sender;
- classification level;
- number of copies;
- designated custodian.

To ensure consistent implementation, the organization establishes a structured workflow covering the entire information lifecycle—from creation to secure destruction. This framework defines key steps, responsible roles, and expected activities to ensure transparency, consistency, and compliance with legal and internal requirements for protecting classified information.

Step	Activity	Responsible Role	Description
1	Creation or receipt of information	Employee / Information creator	Every new piece of information is reviewed to determine whether it contains sensitive or classified data.
2	Sensitivity assessment	Creator + Head of organizational unit	The potential impact of unauthorized access, disclosure, or loss is assessed.
3	Determination of classification level	Authorized person / Manager	The appropriate classification level is assigned (STATE SECRET, TOP SECRET, CONFIDENTIAL, INTERNAL).
4	Marking	Information creator	The information is marked in electronic and/or paper form.

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	Registration and record-keeping	Security Officer / Authorized service	The document, copies, and users are registered and recorded.
6	Storage and access	Information owner + IT department	Measures for physical and technical protection and access control are applied.
7	Use and processing	Authorized users	Information is used only for official purposes and in accordance with the need-to-know principle.
8	Sharing	Authorized person / Security Officer	Sharing is conducted through secure channels and is properly recorded.
9	Reclassification / Declassification	Creator / Authorized person	Periodic reviews are conducted to assess the need for continued classification.
10	Archiving	Archive / Authorized service	Information is retained in accordance with retention periods.
11	Destruction	Authorized commission / Security Officer	Information is securely destroyed and destruction is recorded.

c. Storage, Handling and Control of Classified Information

Classified information shall be stored, processed, and used only under appropriate security conditions and strictly for official purposes, in accordance with legal requirements and established organizational procedures.

The organization establishes an integrated classified information management system covering the following areas:

- **Information Lifecycle Management**

  Procedures are established to manage the full lifecycle of classified information, including:
  - creation and marking of information;
  - secure storage in electronic and physical form;

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

- controlled use and processing;
- controlled sharing and transfer;
- reclassification and declassification where applicable;
- archiving;
- secure disposal and destruction.

➢ **Access and Usage Control**

Measures are implemented to:

- enforce access control based on the **need-to-know** principle;
- prevent unauthorized copying, disclosure, or distribution;
- monitor and control the use of information.

➢ **Control of Digital Channels**

Technical safeguards are implemented to protect electronic information, including:

- encryption of sensitive data;
- use of secure communication channels;
- access control to information systems;
- monitoring and logging of access and information sharing activities.

➢ **Responsibilities and Incident Management**

Roles and responsibilities are clearly defined for:

- the Classified Information Security Officer;
- management;
- employees and information users.

Procedures are established for recording, controlling, and timely reporting of security incidents.

➢ **Training and Awareness**

The organization provides regular training and awareness programs covering:

- proper handling of classified information;
- application of TLP clasiffication;
- compliance with security procedures.

➢ **Control and Audit**

A process is established for regular review and audit of:

- implementation of security measures;
- proper information marking;
- sharing and record-keeping processes.

These activities support organizational maturity and ensure continuous compliance with the legal framework and relevant standards.

d. Reproduction, Translation, and Extracts

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

Reproduction (copying), translation, or creation of extracts from classified information is permitted only when there is an official need and prior authorization.

The following must be ensured:
- control of the number of copies;
- record-keeping of authorized users;
- retention of the original classification level.

e. Dissemination of Classified Information

Information sharing shall be conducted strictly to the extent necessary to achieve the defined operational objective, in accordance with the principle of proportionality and least necessary disclosure.

The sharing of classified information is permitted only:
- in accordance with the **need-to-know** principle;
- to individuals with the appropriate level of authorization;
- in line with the assigned TLP claffication.

All dissemination must be controlled and properly recorded.

f. Transfer of Classified Information

The transfer of classified information must take place through approved and secure channels.

Electronic transfer must include:
- encryption;
- password protection;
- secure communication channels.

g. Removal and Destruction

Classified information must be securely destroyed when no longer required or upon expiry of retention periods.
Destruction methods must prevent:
- reconstruction of information;
- unauthorized access;
- misuse of data.

7. Physical Security

The Ministry of Digital Transformation establishes physical and technical safeguards to prevent unauthorized access to classified information in all facilities and locations where such information is stored, processed, or used.
Physical security aims to:

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

- prevent unauthorized access;
- deter and detect unauthorized activities;
- restrict access in accordance with the need-to-know principle.

a. Areas of Application

Physical security measures apply to:

- organizational buildings and facilities;
- offices and workspaces;
- archives and storage areas;
- server and ICT rooms;
- all locations where classified information is stored or processed.

b. Physical Access Control

The organization implements access control to areas where classified information is handled. Measures include:

- controlled entry and exit;
- identification of employees and visitors;
- visitor escort in secure areas;
- access logs for sensitive premises.

c. Security Zones

Areas where information classified as **CONFIDENTIAL** or higher is stored are designated as security zones.

Enhanced measures in these zones include:

- stricter access control;
- surveillance and protection;
- restriction of unauthorized presence.

d. Technical Protection Measures

Appropriate technical safeguards are implemented in accordance with minimum standards set by competent authorities, including:

- access control systems;
- alarm systems;
- video surveillance;
- locking and facility protection systems;
- protection of server and ICT rooms.

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

e. Need-to-Know Physical Access

Physical access to facilities and information is restricted to individuals with a legitimate business need and appropriate authorization, providing additional protection against unauthorized access and information compromise.

f. Access to Classified Information

Access to classified information is strictly controlled and granted only to individuals and organizations that meet legal requirements and have an official need for access. This principle is a key safeguard against unauthorized use, disclosure, or misuse of classified information.

g. Authorized Users of Classified Information

Authorized users may include:

- state authorities and institutions;
- legal entities established by the state or local government;
- natural and legal persons in the Republic of North Macedonia holding a valid security clearance;
- foreign government authorities, institutions, or legal entities with a valid security clearance and access authorization issued by the competent authority.

h. Security Clearance

Access to classified information is granted only to individuals who:

- hold an appropriate security clearance;
- are authorized to access the relevant classification level;
- are formally approved by the organization.

i. Need-to-Know Principle

Even when an individual holds a valid security clearance, access to specific information is granted only when required to perform official duties.

This principle ensures:

- access is limited to the minimum necessary scope;
- reduced risk of information compromise;
- clear accountability for information use.

j. Access Approval Procedure

The organization establishes procedures for approval, recording, and review of access to classified information to ensure control and traceability of information usage.

k. Institutional Obligations Regarding Security Clearances

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

In accordance with the Law on Classified Information, access to classified information may be granted only to individuals who hold an appropriate security clearance and have an official need for access.

l. Security Clearance Requirement

Employees whose roles and responsibilities require access to classified information must obtain an appropriate security clearance issued by the competent authority.

Security clearance is required in particular for:

- employees within the Cybersecurity Department;
- members of the Government CERT/CSIRT;
- individuals handling classified information;
- individuals involved in incident management;
- individuals authorized to exchange sensitive information with national and international partners.

The level of security clearance is determined based on job responsibilities and the classification level of the information handled.

m. Training Requirement

Individuals with access to classified information must complete appropriate training covering:

- handling of classified information;
- application of the need-to-know principle;
- use of the Traffic Light Protocol (TLP);
- procedures for responding to security incidents.

n. Institutional Obligation to Establish Protective Measures

State and local authorities, legal entities established by the state or municipalities, as well as other legal entities, are obligated to:

- Create the necessary conditions to protect classified information;
- Implement measures to mitigate adverse consequences in the event of classified information disclosure;
- Establish an effective and coordinated system for managing classified information;
- Appoint a security officer responsible for coordinating and supervising the implementation of protective measures.

The objective is to ensure that all activities involving classified information are conducted securely and in compliance with legal obligations.

o. Classified Information Security Officer

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 Ministry of Digital Transformation appoints a Classified Information Security Officer in accordance with the Law on Classified Information and relevant secondary legislation. The Security Officer serves as the central coordination and oversight point for the institution's classified information protection system.

p. Responsibilities of the Security Officer

The Security Officer is responsible for:

- coordinating the implementation of administrative, physical, and technical protection measures;
- recording and reporting incidents related to classified information;
- monitoring the application of the **need-to-know** principle when granting access;
- overseeing the proper handling, storage, and sharing of classified information;
- coordinating training and awareness activities;
- preparing and monitoring annual plans and activities related to the protection of classified information;
- cooperating with competent state authorities in the field of classified information protection.

8. Handling Information Received from FIRST and Other CSIRTs

The Ministry of Digital Transformation, through its CSIRT team, participates in national and international information exchange related to cybersecurity incidents, threats, vulnerabilities, and mitigation measures.

Information received from the FIRST community, other national and international CSIRT/CERT teams and trusted partners and collaborators, shall be treated as sensitive operational information and handled with enhanced confidentiality and protection measures, in accordance with this policy, the application of the Traffic Light Protocol (TLP), and the "need-to-know" principle.

a. Retention of Markings and Restrictions

Any information received from FIRST or another CSIRT team shall:

- retain the original TLP classification.
- not be reclassified without the consent of the source;
- not be shared beyond the scope permitted by the assigned TLP marking.

If the information contains additional restrictions or conditions for use and sharing, such restrictions shall take precedence and must be strictly respected.

b. Handling Information Without a TLP Marking

If information is received without a clearly defined TLP clasiffication, the CSIRT shall:

- assess the sensitivity of the information;
- assign an appropriate TLP classification before further use or sharing;
- treat the information as at least **TLP AMBER+STRICT** until its status is determined.

c. Internal Use and Access Restriction

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 received from FIRST and other CSIRT teams may be shared internally only:

- with personnel who have an official need for access;
- to the extent necessary to perform assigned duties;
- in accordance with the **need-to-know** principle.

Access to such information shall be restricted to the minimum number of authorized personnel required.

d. Restrictions on Further Sharing

Information received from FIRST and other CSIRT teams shall not be shared with:

- the public;
- the media;
- unauthorized persons or organizations, unless:
- the source has provided explicit consent; or
- the TLP classification permits such sharing.

When information is further shared, the following must always be preserved:

- the original TLP classification;
- the source of the information;
- all restrictions defined by the source.

e. Record Keeping and Traceability

The CSIRT shall maintain records of:

- the receipt of information from FIRST and other CSIRT teams;
- its processing and use;
- any further sharing, when permitted.

These records shall be maintained to ensure confidentiality, accountability, and traceability within the information-sharing process.

9. Handling Classified and Sensitive Information on Portable Devices and Outside Official Premises

To mitigate the risk of unauthorized access, loss, or compromise of information, the Ministry establishes rules for the use of portable devices and the processing of information outside official premises.
These rules apply to:

- Official laptops;
- Mobile phones;
- Tablet devices;
- Remote work and work from home;
- Access to official information via external networks.

a. Fundamental Principles

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

Classified and sensitive information may only be processed outside official premises when necessary for the performance of official duties and in compliance with appropriate technical and organizational protective measures.
The use of personal devices for processing classified information is strictly prohibited.

b. Storing Information on Portable Devices

For official laptops and mobile devices:

Information marked TLP RED and TLP AMBER+STRICT:

- Must not be permanently stored locally without prior authorization;
- Must be protected with encryption;
- Must be stored exclusively in approved information systems;
- Must be secured with authentication and access control mechanisms.

Information marked TLP GREEN:

- May be processed on official devices with standard security measures applied.

Information marked TLP CLEAR:

- May be processed without additional restrictions.

Remote Work and Use of External Networks

When accessing official systems from external networks, the following must be applied:
- Use of secure VPN connections;
- Multi-factor authentication;
- Use of official devices only;
- Avoidance of public or unsecured wireless networks.

Processing classified information in public locations (airports, hotels, public spaces) must be avoided unless strictly necessary and should be conducted with heightened caution.

Communication via Mobile and Unsecured Channels

Information marked TLP RED and TLP AMBER+STRICT must **not**:
- Be discussed via personal mobile phones;
- Be transmitted through unsecured communication applications;
- Be shared via personal email accounts;
- Be processed through non-official communication channels.

Sensitive information must be communicated exclusively through:
- Approved official communication channels;
- Secure communication platforms;

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

- Official email with applied security measures.

Protection in Case of Device Loss or Theft

In the event of loss or theft of an official device, the user must immediately notify the responsible ICT sector and the security officer.

The Ministry implements measures to:
- Remotely lock or erase data;
- Prevent unauthorized access;
- Record and analyze the incident.

10. Disclosure of Information and Public Communication by CSIRT

To ensure transparency, trust, and a coordinated response to cyber incidents, the Ministry establishes rules for the disclosure of information by the CSIRT team to the public, affected parties, and partner organizations.

Information disclosure must comply with:
- The applicable legal framework;
- The "need-to-know" principle;
- The application of TLP (Traffic Light Protocol);
- Confidentiality obligations towards reporters and partners.

Authorization for Public Statements

Public statements, press releases, and information related to cybersecurity incidents may only be issued:
- By authorized personnel;
- Through the institution's official communication channels.

CSIRT team members must not independently provide statements to the media or public without prior approval from management.

Information Permitted for Public Disclosure

Information may be publicly disclosed if it:
- Is marked TLP CLEAR;
- Is aggregated and anonymized;
- Constitutes warnings, recommendations, or security guidance;
- Aims to raise public awareness;
- Does not allow identification of affected organizations or individuals.

Information Prohibited from Public Disclosure

The following information must **not** be publicly disclosed:
- Details of ongoing or active incidents;

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

- Technical information that could be misused;
- Information that could identify victims;
- Data obtained from other CSIRT teams without their consent;
- Information marked TLP:RED or TLP:AMBER+STRICT.

a. Communication with Affected Organizations (Incident Victims)

CSIRT ensures confidential and controlled communication with organizations and individuals affected by incidents.

When communicating with affected parties:
- Only information necessary to mitigate and resolve the incident is shared;
- The confidentiality of reporters is respected;
- Information is not shared with third parties without consent, unless legally required.

Affected parties may expect that information provided will be used exclusively for incident handling and coordination.

b. Sharing Information with Other CSIRT Teams

CSIRT may share information with other national and international teams when necessary to:
- Prevent or mitigate incidents;
- Coordinate threat response;
- Protect critical infrastructure.

Information sharing must always comply with:
- TLP restrictions;
- Agreements and confidentiality obligations;
- Legal requirements.

c. Public Availability of Restrictions

The Ministry ensures public accessibility of the core principles for confidentiality and information disclosure, so that affected parties and partners have clear expectations regarding the handling of provided information.

11. Confidentiality of Information Provided by Incident Reporters

CSIRT ensures the confidential handling of all information submitted by organizations, institutions, and individuals when reporting cyber incidents, vulnerabilities, and threats.

The objective is to build trust and encourage timely reporting of incidents.

a. Principle of Reporter Confidentiality

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 received during incident reporting is considered confidential and is used exclusively for:

- Analysis and processing of the incident;
- Coordination of response efforts;
- Prevention of further harm;
- Enhancement of national cybersecurity.

The identity of the reporter will not be disclosed without prior consent, except when legally required.

b. Restricted Access to Submitted Information

Access to information provided by reporters is limited to:

- CSIRT team members;
- Authorized personnel within the institution when necessary for incident handling;
- Competent authorities when legally mandated.

All individuals with access to this information are required to maintain its confidentiality.

c. Sharing Information with Third Parties

Information provided by reporters may only be shared with third parties when:

- Necessary for incident resolution;
- Legally required;
- Prior consent has been obtained from the reporter;
- Information is anonymized and does not allow identification.

d. Anonymization and Aggregation of Data

CSIRT may use aggregated and anonymized data for:

- Statistical analysis;
- Reporting;
- Public awareness initiatives;
- Improving protective measures.

Such data must not allow the identification of the reporter or affected organization.

e. Reporter Expectations

Organizations and individuals reporting incidents may expect that:

- Their information will be treated as confidential;
- Information will not be publicly disclosed without justification;
- CSIRT will act in accordance with principles of trust, professionalism, and legality.

13. Publicly Available Restrictions on Information Disclosure

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

To ensure transparency and clear expectations among stakeholders, the Ministry publishes the core principles and limitations related to information disclosure by CSIRT.

These restrictions are publicly available to build trust and encourage cooperation in the reporting and handling of cyber incidents.

f. Information CSIRT May Disclose

CSIRT may publicly disclose information that:

- Is marked TLP CLEAR;
- Is aggregated and anonymized;
- Relates to trends, statistics, and general threats;
- Provides security warnings and recommendations;
- Does not allow identification of affected organizations or individuals;
- Does not jeopardize the ongoing handling of incidents.

g. Information CSIRT Does Not Disclose

CSIRT does not publicly disclose:

- Information marked TLP:RED or TLP:AMBER+STRICT;
- Information about ongoing or unresolved incidents;
- Technical details that could be misused;
- The identity of affected organizations or individuals;
- Information received from other organizations or CSIRT teams without their consent;
- Information subject to legal restrictions or classification.
-

h. Disclosure Limitations

The disclosure of information may be restricted when:

- There is a risk to national security;
- There is a risk of additional harm or misuse;
- The information is part of an ongoing investigation;
- Contractual or legal confidentiality obligations apply.

i. Purpose of the Restrictions

These restrictions aim to:

- Protect affected stakeholders;
- Prevent additional cyber threats;
- Maintain trust with partners;
- Ensure compliance with legal and international obligations.

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

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