Information Disclosure Policy

Version 1.0 – 16.03.2016

Document classification: PUBLIC / TLP WHITE

Contents

1. Introduction

The processing of sensitive information is an important aspect in the daily operations of the National Centre for Computer Incident Response, hereinafter: MKD-CIRT. Sensitive information can be received in the MKD-CIRT through an incident report submitted by a constituent or another party that is participating in the process of incident management. Maintaining the confidence in the ability of MKD-CIRT to protect sensitive information is essential for its operation. The rules on disclosure of information described in this document are intended to help the MKD-CIRT in maintaining a high level of confidence.

1.1. Objective

This policy defines and describes the principles followed by MKD-CIRT when disclosing, publishing and sharing of information, and along with the Information Classification Policy of MKD-CIRT is designed to maintain the confidentiality of data used by MKD-CIRT.

1.2. Scope

This policy covers all information assets created, managed, transferred or recorded by MKD-CIRT.

1.3. Links and references

- Information classification policy of MKD-CIRT
- Form: Authorization for information disclosure
- Form: Non-disclosure agreement
- Law on Personal Data Protection
- Law on Electronic Communications
  Law on Classified Information

1.4. Abbreviations

Abbreviation	Description
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIRT	Computer Incident Response Team
CSIRT	Computer Security Incident Response Team
TLP	Traffic Light Protocol

2. Definitions

2.1. Information exchange

Information exchange shall mean "exchange of information" that may be done in person, e.g. during meetings with CSIRT teams or between MKD-CIRT and its constituents, or at a meeting attended by experts on information security; it can also be in the form of exchange of messages via e-mail or telephone conversion.

2.2. Anonymization

Anonymization shall mean deleting the user identification properties.

3. Responsibility for data management

All members of MKD-CIRT shall have an obligation to protect the confidentiality of the data with which they work, regardless of form or medium on which the data is stored or transmitted, according to the operating procedures of MKD-CIRT.

MKD-CIRT shall be responsible for the implementation of appropriate procedural, physical and technical controls of access, use, transfer or disposal of data in the possession of or used by MKD-CIRT in accordance with this policy.

In order to avoid any leaks of sensitive information, MKD-CIRT members will disclose the information only if necessary and in accordance with the following rules.

4. Disclosure of information

4.1. Protection of Information

When exchanging information, MKD-CIRT shall use the "need to know" principle: Information that is not public MUST NOT be publicly shared, and MUST ONLY be shared with the entities that need to know it.

The information will be disclosed and shared in accordance with the original level of confidentiality.

MKD-CIRT shall respect the assigned classification of the information given by the source that has submitted the information to MKD-CIRT in accordance with the internal operating procedures of MKD-CIRT.

Disclosure and publication of sensitive information will be made ONLY IF NECESSARY to resolve the incident. In item 3.3. - Anonymization outlines the principles of MKD-CIRT on disclosure of information of this kind.

MKD-CIRT often collaborates with several groups, including other CSIRT teams and stakeholders, producers and suppliers, enforcement authorities and others. Disclosure of information to these groups will be conducted on an individual basis and commensurate to the risk of information disclosure. MKD-CIRT shall reserve the right to ask for signing a non-disclosure agreement prior to disclosing information.

Before the exchange of confidential information with other partners, often other CSIRT teams involved in the investigation of the computer security incident, the honesty of these parties shall be confirmed.

When communicating with other CSIRT teams and third parties, MKD-CIRT will ensure that information made available to others:

- is signed to ensure non-repudiation, and
- is encrypted to protect the confidentiality, whenever necessary, in accordance with this policy.

4.2. Personal data protection and legal aspects

MKD-CIRT will submit the requested information to state bodies, public institutions or authorized third parties whenever there is a legal obligation thereto. However, MKD-CIRT will do so only after all legal requirements have been met, e.g. delivery of a court order.

Any case of processing or transmission of personal data as per its form and content will be in accordance with the Law on Personal Data Protection, Law on Classified Information, Law on Electronic Communications, and other valid regulations in Republic of Macedonia, taking into account the policies and decision on information classification of NATO and the European Union.

4.3. Anonymization

Sensitive information will be first anonymized, before shared with a third party. Personal information (which can be used to identify the purpose of the computer attack or any individual) or additional data shall not be shared without an explicit written consent of the data owner or without adequate data anonymization. This information may be disclosed to third parties only if necessary for resolving the incident.

When the anonymization of the information is not practical or counter-productive in relation to handling the incident, MKD-CIRT shall reserve the right to share certain non-anonymized information with groups or third parties with which it has built-up confidence.

These exchanges of information shall be executed in accordance with the applicable laws in the Republic of Macedonia, and with the express written consent from the owner of the information exchanged (Form - Authorization to Disclose Information)

4.4. Using TLP to share information

4.4.1. General principles

In order to protect the information, MKD-CIRT will apply its internal Information Classification Policy of MKD-CIRT. MKD-CIRT Team, when exchanging information, will apply certain rules that are based on the use of generally accepted and used TLP protocol - Traffic Light Protocol.

MKD-CIRT will mark the information exchanged with an appropriate designation in accordance with TLP, only when exchanging information with a party that has accepted the use of this protocol. If this protocol is not supported by the party with whom the information is exchanged, MKD-CIRT will verify and align the levels of classification applied by both parties, before the information is shared.

The rules for classification of information in accordance with the TLP protocol are given in the Appendix - Using TLP (Traffic Light Protocol) to share information.

Any communication and exchange of information at a level higher than GREEN, and especially e-mails, will be marked with the symbol "[TLP Colour]," where colour can have any value RED or AMBER.
Similar mark or stamp has to be clearly visible on the cover or title of the documents sent or published by MKD-CIRT. If the communication is conducted via telephone or video conference, the appropriate level for classification of information in accordance with the TLP should be stated at the beginning of the conversation, before the delivery of the information.

4.4.2. Standard TLP level of classification

Standard TLP classification level used for information disclosure will be [TLP AMBER] information disclosure level.

Appendix - Using TLP (Traffic Light Protocol) to share information

Any information exchanged will be always marked with a designation in accordance with the following table. If the information exchanged is not marked, MKD-CIRT will mark it with a TLP AMBER designation:

Designation	Use explanation
TLP RED	Information that is not disclosed and is restricted only to the participants in the information exchange. The participants shall not be allowed to share the information outside the participants of this information exchange. Information marked with level TLP RED may be discussed only during the exchange of this information, when all the participants of the information exchange have agreed thereto. Persons or parties, who are not participants in the TLP RED information exchange, MUST NOT attend the information exchange or discussion.
TLP AMBER	The information has a restricted disclosure and is intended only for the participants of the information exchange, members of organizations or constituents (direct employees, consultants, or other relevant professionals) who have fulfilled the "NEED TO KNOW" requirement in order to be able to act upon the information.
TLP GREEN	Information can be shared with other organizations, while sharing information with individuals and experts in the field of information security, but it must not be made public, nor placed on a public web-site.
TLP WHITE	Public information, there are no restrictions in its dissemination, publication, placement on public web-sites or broadcasting. Any participant of the information exchange may publish the information observing the rights to intellectual property protection.