Republic of North Macedonia

Ministry of Digital Transformation

CODE OF ETHICAL CONDUCT FOR MKD-GOV-CSIRT

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

These rules of ethical conduct are adopted in accordance with the Law on Security of Network and Information Systems and in line with comply with the requirements of Directive (EU) 2022/2555 (NIS2). They constitute an integral part of the institutional framework for the functioning of the Government Computer Security Incident Response Team (MKD-GOV-CSIRT), aimed to ensure confidentiality, professionalism, integrity and transparency in its actions.

1.Purpose and Scope

This document defines the principles and standards for ethical behavior of MKD-GOV-CSIRT, with the aim of:

- Alignment with the SIM3 maturity model;
- The rules are aligned with the FIRST (Forum of Incident Response and Security Teams) Code of Ethics and serve as an internal document to support the membership and active participation of MKD-GOV-CSIRT in the FIRST community;
- MKD-GOV-CSIRT acts in good faith and in the interest of national and global cybersecurity, in accordance with the principles of the FIRST community.

The document applies to all employees, collaborators and contracted experts working under the authority of MKD-GOV-CSIRT. This framework includes principles formulated as statements of responsibility, based on the understanding that the public good is always the primary concern. Each principle is supplemented by guidelines, which provide explanations to help computer professionals understand and apply the principle.

2.Fundamental Ethical Principles (FIRST Code of Ethics)

MKD-GOV-CSIRT accepts and implements the following duties that are in accordance with the basic ethical principles of FIRST (Code of Ethics):

2.1 Duty of trust and cooperation

MKD-GOV-CSIRT actively collaborates with other CSIRT teams and institutions, building relationships based on trust. Trust is the foundation of many relationships between teams and is often required before meaningful information exchange can occur. The FIRST community is built on this trust and can only continue to function in this way if there is a reasonable level of trust between teams.

Trustworthiness means that team members should only:

1) make commitments that they can fulfil;

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

2) behave predictably towards other teams (e.g., adhere to TLP standards);

3) maintain the trust relationship they have with other teams. The trust relationship should be initially assumed and transitory, i.e. Trust on First Use (TOFU) and provide trust for teams that are trusted by other teams.

2.2 Duty to Coordinate Vulnerability Disclosure

Team members who become aware of a vulnerability should work with stakeholders to remediate the security vulnerability and minimize the harm associated with the disclosure. Stakeholders include, but are not limited to: the vulnerability reporter, affected vendors, coordinators, advocates and customers, partners, and users. Team members should coordinate with appropriate stakeholders to agree on clear timelines and expectations for disclosure, providing sufficient detail to allow users to assess their risk and take actionable defensive measures.

2.3 Obligation of Confidentiality

Team members have a duty to maintain confidentiality where appropriate. Requirements to keep certain confidential information confidential may be explicit, for example, with the Traffic Light Protocol (TLP).

Team members should respect such requests whenever possible. If it is not possible to keep them confidential, for example, due to conflicts with local law, contract or duty to inform requirements, the team member should immediately notify the owner of the information of this conflict. Some confidentiality duties are based on law, regulation or custom. If, during an incident response, some parties are obligated or expect confidentiality based on such considerations, they should make every effort to make these expectations explicit in advance.

2.4 Commitment to Acknowledgement

Teams receive information from many different sources: researchers, clients, other teams, government entities, etc. Team members should respond to requests in a timely manner, even if it is just to confirm that the request was received. When possible, team members should set expectations for the next update.

2.5 Duty of Authority

Team members have a legitimate need and right to understand their areas of responsibility, acting only on systems to which they have authority to access. Team members should be aware of how their actions may affect their constituents and ensure that they do not cause further harm while carrying out their duties. Where possible, constituents should be consulted before changes are made to their systems.

2.6 Duty to inform

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

Team members should consider it their duty to inform their constituents of current security threats and risks. When team members have information that could adversely affect or enhance security and safety, they have a duty to inform relevant parties or others who can assist, using reasonable efforts, considering confidentiality, privacy laws and regulations, and other obligations.

2.7 Respect for privacy and human rights

Team members should be aware that their actions may impact the human rights of others through the sharing of information, possible bias in their actions, or the violation of property rights. Team members have access to a wide range of personal, sensitive, and confidential information in the course of responding to incidents. This information should be handled in a manner that respects human rights.

During incident response, responders should not act with bias and should do everything they can to eliminate bias from their processes and decision-making.

For the purposes of this principle, the term "property" (UN Declaration of Human Rights: Article 17) includes intangible assets such as intellectual property, as well as ideas and concepts in general, regardless of whether they are legally protected (e.g., patented).

2.8 Duty to Team Health

Teams have a responsibility to continue to provide the services they have promised to their constituents. This responsibility includes the physical and emotional health of the team. To respect the members who make up the team as individuals and to enable the long-term sustainability of an appropriate level of service, the team should strive to maintain a healthy, safe and positive work environment that supports the physical and emotional health of all its members.

2.9 Team Capacity Development Duty

Incident management is an evolving subject that team members should continually learn. The team should provide resources for its members to learn, apply, and advance technological and scientific knowledge within their area of responsibility. Training or CPE/CEU educational credits may contribute, but compliance exercises alone are not sufficient to fulfill this duty. The team should maintain sufficient technological infrastructure to enable its services, including appropriate measures to protect that infrastructure from interference by external parties.

2.10 Duty to Collect Data Responsibly

Collecting data is essential to incident response, but a balance should be struck between the purpose of the incident response and respect for stakeholders. During an investigation, the amount of information needed to be collected may change. As the incident is being worked on, team members should adjust what they collect as needs change. Data that is not directly relevant to the incident and its remediation should be excluded from reporting.

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

Before sharing data with third parties for mitigation, the risks should be weighed against the benefits. Data should only be shared if the benefits clearly outweigh the risks. Sensitive data should be stored in a manner that can be easily destroyed after the incident has been resolved. Collected data should be securely destroyed in accordance with data retention policies.

2.11 Duty to respect legal and institutional jurisdictions

Team members should recognize and respect the legal and institutional competencies, legal rights, rules, and authorities of parties involved in incident response activities.

Laws, regulations, and other legal issues, such as those related to privacy or data breach notification, may vary between different legal systems, countries or sectors. Competencies may be determined by the physical locations of the parties involved, such as their countries or residences, as well as other factors that apply to those parties. Even within a country, laws and regulations may differ between political regions (e.g., between individual states in the United States) or between different businesses, industries, or sectors within that nation (e.g., healthcare, financial services, and government facilities). National CSIRTs may have designated responsibilities and/or authority for activities involving components within their own jurisdiction, and they may also collaborate with or "hand off" information and activities to other entities that have jurisdiction over jurisdictions that cross borders.

Team members should be aware of key issues affecting the jurisdictions involved, including but not limited to privacy regulations or data breach notification requirements. As cybersecurity and privacy laws and regulations evolve and continue to be updated around the world, it is advisable to consult knowledgeable legal counsel for guidance whenever issues involve multiple legal or institutional competencies.

2.12 Duty to exercise judgment based on evidence and facts

Teams should operate based on verifiable facts. When sharing information, such as indicators of compromise (IOCs) or incident descriptions, team members should transparently provide evidence and scope. If this is not possible, the reasons for not sharing this evidence and scope should be stated with the information.

Team members should refrain from spreading or sharing rumours. Any hypothesis should be clearly identified as such.

Transparent processes of evidence and reasoning are important even in the case of automated sharing, e.g., during automated sharing of large amounts of information. In this case, a description of the data collection process should be communicated at an understandable level of detail.

3. Dealing with dilemmas

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

Team members can often find themselves in a position where no action satisfies all ethical principles. In such a situation, a choice must be made about which principles to prioritize. In this situation, incident responders are encouraged to consider which stakeholders might be affected by their actions and how, preferably in discussion with a colleague. As a rule, the solution that minimizes the violation of this ethical framework should be chosen. Sometimes, this may not be possible, e.g. due to external pressures. In such a situation, it is recommended to proceed, keeping the ethical dilemma in mind.

4. SIM3 Model Compliance

MKD-GOV-CSIRT:

- Applies this regulation together with P11 – Internal document for secure information management and other related policies for information protection and processing;
- Maintains formal incident management procedures in accordance with the SIM3 domains: Organization, People, Processes and Tools;
- Ensures clear roles and responsibilities;
- Implements confidentiality, integrity and availability controls;
- Documents activities for audit and improvement purposes.

5. Practical rules of conduct

- Unauthorized disclosure of information is prohibited.
- Use of confidential data for personal gain is prohibited.
- Any conflict of interest must be reported immediately.
- All activities must be documented and audited

6. Training and Awareness

MKD-GOV-CSIRT provides regular training on:

- FIRST Code of Ethics;
- SIM3 controls;
- TLP proper implementation;
- protection of personal data and classified information.

7. Non-compliance and sanctions

Breach of these rules may result in disciplinary, misdemeanour or other liability, in accordance with applicable national legislation.

8. Review and improvement

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 document is revised at least annually or following changes in FIRST standards, the SIM3 model or legislation.

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