RFC2350 – Description of NCSC-MD of Moldova

1. Document Information

This document contains a description of NCSC-MD in accordance with RFC2350, providing basic information about the NCSC-MD team, its channels of communication, its roles and responsibilities.

1.1. **Date of Last Update**:
This is version 1.0. This document was last updated on **15.04.2025**.

1.2. **Distribution List for Notifications**:
Subscribers to the **NCSC-MD of Moldova** mailing list will receive notifications of updates.
Subscription requests can be sent to **csirt@asc.gov.md**.

1.3. **Locations where this Document May Be Found**:
The latest version of this document is available at:
https://asc.gov.md.

1.4. **Authenticity of this Document**:
This document has been digitally signed by the **Agency for Cyber Security** Director and by the **NCSC-MD of Moldova** Deputy Head using their digital signatures.

---

2. Contact Information

2.1. **Name of the Team**:
National CSIRT of Moldova

2.2. **Mailing Address**:
Puskin Street 26
Chisinau, Republic of Moldova
Postal code 2012

2.3. **Time Zone**:
Eastern European Time (EET), GMT+2
During daylight savings time: GMT+3

2.4. **Telephone Number**:
+373 696 32 800

2.5. **Facsimile Number**:
Not available

2.6. **Other Telecommunication**:
Not available

2.7. **Electronic Mail Address**:
csirt@asc.gov.md

2.8. **Public Keys and Encryption Information**:
The **National CSIRT of Moldova** uses PGP for secure communications. The public key can be found at:
https://keys.openpgp.org/vks/v1/by-fingerprint/7C3C24A84914A2FF42E4A7624A500AA5D70A0444
Fingerprint: **[7C3C 24A8 4914 A2FF 42E4 A762 4A50 0AA5 D70A 0444]**

2.9. **Team Members**:
Radu VIERU is Deputy Head of National CSIRT of Moldova.
Team members include security analysts, incident responders, and cybersecurity experts.

2.10. **Operating Hours**:
Normal operating hours are Monday to Friday from 08:00 to 17:00.
For critical incidents, a 24/7 response is available via the emergency contact line.

2.11. **Additional Contact Information**:
For urgent incidents, please contact the 24/7 hotline: +373 696 32 800

---

3. Charter

3.1. **Mission Statement**:
The **National CSIRT of Moldova** is responsible for coordinating the prevention, detection, and response to cybersecurity incidents affecting Moldova's critical infrastructure, government institutions, and national entities. Its mission is to ensure the resilience and security of Moldova's cyberspace by providing timely incident handling, vulnerability coordination, and cybersecurity threat intelligence.
By performing the function of cyber incident response team, NCSC-MD:
a) coordinates the process of ensuring cybersecurity, preventing and resolving cyber incidents;
b) monitors, analyses and, if necessary, prepares reports on cyber threats, cyber vulnerabilities and incidents at the national level;
c) upon request, assists service providers in the process of monitoring and protecting their information networks and systems;
d) receives notifications of cyber incidents;
e) ensures response to cyber incidents and provides assistance to service providers in this regard;
f) collaborates nationally and internationally with cyber incident response teams, including through the cyber incident management platform and for information sharing purposes;
g) manages cybersecurity crises at the national level in accordance with the national cyber incident and crisis response plan;
h) ensures registration of cyber incidents.

3.2. **Constituency**:
The **National CSIRT of Moldova** serves:

- Government agencies
- Critical infrastructure operators
- Financial institutions
- Internet Service Providers (ISPs)
- Private sector organizations
- The general public

NCSC-MD is national single point of contact of Moldova cyber domain.

3.3. **Sponsorship and/or Affiliation**:
The **National CSIRT of Moldova** operates under the authority of the **Ministry of Economic Development and Digitalization** and is affiliated with regional and international CSIRTs.

3.4. **Authority**:
The **National CSIRT of Moldova** operates under the mandate of the **LAW Nr. 48 from 16-03-2023 regarding to Cyber Security**, which grants authority to manage and respond to cybersecurity incidents within Moldova's national boundaries.

---

4. Policies

4.1. **Types of Incidents and Level of Support**:
The **National CSIRT of Moldova** handles a wide range of cybersecurity incidents, including but not limited to:

- Denial of Service (DoS) attacks
- Data breaches
- Phishing and social engineering attacks
- Malware and ransomware infections
- Network intrusions
- System compromises
- Vulnerability management and coordination

The level of support provided will vary based on the severity of the incident, the affected entities, and the potential impact on national security and critical services.

4.2. **Cooperation, Interaction, and Disclosure of Information**:
The **National CSIRT of Moldova** cooperates with other CSIRTs, law enforcement agencies, private sector partners, and international organizations to share relevant incident information in accordance with confidentiality agreements and legal obligations. Incident information may be shared with:

- Other CSIRTs (regional, global)
- Law enforcement agencies
- Affected organizations
- Government authorities

NCSC-MD is a listed member of TF-CSIRT community and cooperates with other CSIRTs.

4.3. **Communication and Authentication**:
All sensitive communication will be encrypted using PGP. When sharing critical information, mutual authentication methods will be employed to ensure the integrity and confidentiality of the data exchanged.

---

5. Services

5.1. **Incident Response**
The **National CSIRT of Moldova** handle the technical aspects, therefore **NCSC-MD** provides the following incident response services:

5.1.1. **Incident Triage**

- Receive and analyze incident reports
- Verify the occurrence and nature of incidents (based on ENISA Reference Incident Classification Taxonomy)
- Prioritize incidents based on their severity and impact

5.1.2. **Incident Coordination**

- Determining the involved organization
- Coordinate response efforts with affected organizations, other CSIRTs, and stakeholders
- Disseminate incident-related information to relevant parties

5.1.3. **Incident Resolution**

- Provide technical assistance to resolve incidents
- Work with system administrators to remediate vulnerabilities and restore affected systems

5.2. **Proactive Services**
In addition to incident response, the **National CSIRT of Moldova** offers proactive services, including:

- Vulnerability management and disclosure
- Threat intelligence sharing
- Security awareness and training programs
- Regular advisories and alerts

---

6. Incident Reporting Forms

Incident reporting forms can be found on our website at **https://asc.gov.md.**
Please complete the form with as much detail as possible to help us efficiently handle the incident.

---

7. Disclaimers

While the **National CSIRT of Moldova** endeavors to provide timely and effective incident response services, it is not liable for any damage or loss caused by security incidents. All advice and assistance are provided on a best-effort basis.

---

8. Additional Information

Further information about the **National CSIRT of Moldova** and its services is available on our website:
https://asc.gov.md
For urgent matters, contact our 24/7 hotline: +373 696 32 800.