RFC 2350 - MVR-SOC

Cybersecurity Unit of the Ministry of Interior

Introduction **Contact Information** **Charter** **Policies** **Services** **Incident Reporting** **Disclaimer**

1. Introduction

This document outlines the operations of the Cybersecurity Unit (MVR-SOC) of the Ministry of Interior in accordance with RFC 2350. It details the SOC's mission, services, and procedures for handling security incidents.

1.1 Overview

Version 1.0 - 22.07.2025

1.2 Distribution List for Notifications

Changes to this document will be announced via the Ministry of Interior's SOC website at https://www.mvr.gov.mk/cybersecurity. Changes are not disseminated via mailing lists, RSS feeds, or other automated distribution mechanisms.

1.3 Locations where this Document May Be Found

The current version of this document is always available at https://www.mvr.gov.mk/cybersecurity.

1.4 Authenticating This Document

This document is signed with the MVR-SOC's PGP key. The public key is available at https://www.mvr.gov.mk/cybersecurity.

2. Contact Information

2.1 Name of the Team

English: Cyber Security Unit of the Ministry of Interior

Macedonian: Одделение за сајбер безбедност на Министерството за внатрешни работи

Short name [EN]: MVR-SOC

Short name [MK]: МВР-SOC

2.2 Address

Ministry of Interior
Ul. Dimche Mirchev 9
1000 Skopje
Republic of Macedonia

2.3 Time Zone

CET

2.4 Telephone Number

Working hours: +389 (0)72 334 012
Emergency phone: +389 (0)2 3117 222

2.5 Facsimile Number

N/A

2.6 Other Telecommunication

Internet Website: https://www.mvr.gov.mk

2.7 Electronic Mail Address

soc@moi.gov.mk

2.8 Public Keys and Encryption Information

The e-mail address (soc@moi.gov.mk) used by MVR-SOC shares the same PGP key:

- **Key Id:** 0 x C06C0A5B
- **Key Type:** RSA 4096
- **Key Fingerprint:** 6367 3F63 C8BC A7F1 69C1 15C4 4536 1E5D C06C 0A5B

  Public key https://www.mvr.gov.mk/cybersecurity

The public key and its signatures can be found on public key servers and at https://www.mvr.gov.mk/cybersecurity. This key signs all MVR-SOC communications and is used for confidential communication (incident reports, alerts).

2.9 Team Members

The full list of MVR-SOC team members is not publicly available. Team members will identify themselves with their full name in official communications regarding incidents.

2.10 Other Information

N/A

2.11 Points of Customer Contact

The preferred method to contact MVR-SOC is via e-mail at soc@moi.gov.mk, monitored 24/7 by a duty officer.

Working hours phone: +389 (0)72 334 012
Urgent cases can be reported 24/7 by phone at +389 (0)2 3117 222.

Hours/Days of Operation: 08:00 to 16:00, Monday to Friday (except holidays). Out-of-office hours support is available for emergencies.

3. Charter

3.1 Mission Statement

The mission of MVR-SOC is to safeguard and support the ICT systems of the Ministry of the Interior, ensuring the confidentiality, integrity, and availability of all data within its infrastructure. MVR-SOC monitors, detects, responds to, and recovers from both intentional cyber threats and unintentional incidents that may compromise the Ministry's ICT assets or impact Macedonian citizens.

3.2 Constituency

The constituency of MVR-SOC includes employees and ICT systems of the Ministry of Interior.

3.3 Sponsorship and/or Affiliation

MVR-SOC is part of the Ministry of Interior.

3.4 Authority

The establishment of the SOC is mandated by the Rulebook on the Organization of the Ministry of the Interior.

4. Policies

4.1 Types of Incidents and Level of Support

All cybersecurity incidents are assigned a normal priority level unless explicitly classified as EMERGENCY or URGENT.

4.2 Co-operation, Interaction and Disclosure of Information

MVR-SOC prioritizes operational cooperation and information sharing with other cybersecurity teams (SOCs and CIRTs) and organizations to enhance cybersecurity. All information is handled with strict confidentiality. Unless otherwise agreed, shared information is considered sensitive and disclosed only to parties directly involved in incident investigation and resolution. The Traffic Light Protocol (TLP) is used to classify and manage information sensitivity.

MVR-SOC operates in accordance with the Macedonian legal and regulatory framework.

4.3 Communication and Authentication

Email and telephone communications are secure for low-sensitivity information without encryption. Highly sensitive data exchanges use encryption methods like PGP. Identity verification, when required, is performed through established webs of trust or alternative methods.

5. Services

5.1 Incident Response

MVR-SOC supports local network and system administrators in managing cybersecurity incidents.

- **Incident Triage:** Assessing the scope, priority, and impact of incidents, identifying initial resources needed.
- **Incident Coordination:** Mobilizing internal resources, reaching out to external parties for assistance, and notifying affected or endangered parties.
- **Incident Resolution:** Providing guidance on response actions, assisting in evidence collection for cyber-crime and forensic departments, and deploying on-site when necessary.

5.2 Proactive Activities

MVR-SOC processes Indicators of Compromise (IoCs) and disseminates relevant information to responsible contacts for affected systems. Activities include network and log analysis, threat intelligence monitoring, and vulnerability assessments. MVR-SOC issues announcements, warnings, and alerts to its constituency and contributes to improving security awareness.

5.3 Reactive Activities

MVR-SOC coordinates with external entities and prepares post-incident reporting with recommendations.

6. Incident Reporting Forms

No formal incident reporting form is available at this time.

7. Disclaimer

While every precaution is taken in preparing information, notifications, and alerts, MVR-SOC assumes no responsibility for errors, omissions, or damages resulting from the use of the information contained within.