Ver.: 0.1

Date: 16 April 2026 12:38, +0200 EET

1. Document Information
This document contains a description of MFA (Ministry of Foreign Affairs of the Republic of Lithuania) according to RFC 2350. It provides basic information and functions about the MFA: contacts, responsibilities, services offered.
1.1. Date of last update
16 April 2026 12:38, +0200 EET
1.2. Distribution List for Notifications
There is no distribution list for notifications.
1.3. Locations where this document may be found
The current version of this MFA LT CERT description document is available in the organization's document management system: https[:]//avilys.int.urm.lt/ and public website https[:]//www.urm.lt/en/about-us/organisation/contact-information/938
1.4. Authenticating this Document
The English version of this document is registered in the organization's document management system and signed.
2. Contact information
2.1. Name of the team
In order to strengthen resilience against growing threats and ensure the security of diplomatic relations, preparations were carried out and decisions were taken in 2022 at the Ministry of Foreign Affairs of the Republic of Lithuania regarding the establishment of a specialized cybersecurity unit.
2.2. Address
J. Tumo-Vaižganto St. 2, LT-01108 Vilnius
2.3. Time zone
-EET, Eastern European Time (UTC+2, between last Sunday in October and last Sunday in March) -EEST, Eastern European Summer Time (UTC+3, between last Sunday in March and last Sunday in October)
2.4. Telephone number
+370 664 85342
2.5. Facsimile number
+370 5 236 2626
2.6. Other telecommunication
+370 5 236 2444
2.7. Electronic mail address
<CERT_URM (at) urm.lt > This e-mail forwards information to the specialists on duty at MFA LT CERT.
2.8. Public keys and encryption information
-----BEGIN PGP PUBLIC KEY BLOCK----- Comment: Fingerprint: 034D71AA28A3B1E918ED46E92C7BDB3157924E49 mDMEaczkZBYJKwYBBAHaRw8BAQdAfWCUvkz6avIievJLWtZGOQCgOFW/I+Q1MACo vQzGiqe0GkNFUlQgVVJNIDxjZXJ0X3VybUB1cm0ubHQ+iJkEExYKAEEWIQQDTXGq KKOx6RjtRukse9sxV5JOSQUCaczkZAIbAwUJBaTmLAULCQgHAgIiAgYVCgkICwIE FgIDAQIeBwIXgAAKCRAse9sxV5JOSRC+AP98orVVTt/Oq6Q/6Dp51swWupG6HXvx UKndaxE+5i3S6AEA4PFNjditwiS97vYaLwlyRw+/I1VgcsPrbr+qotoMmgi4OARp zORkEgorBgEEAZdVAQUBAQdAz20N6/0F2uekYjGQ2JP0S3QIjk12BUVQGlcGZEvq

M10DAQgHiH4EGBYKACYWIQQDTXGqKKOx6RjtRukse9sxV5JOSQUCaczkZAIbDAUJ
BaTmLAAKCRAse9sxV5JOSUXjAP9anRurEQTfbjK0Ex86i940nQkZUkR/yoUkEp3j
JQt01gD/QJHZtlYASkHdeiXupUo0n/5Yp+BKL9fBWYHQdhwqoAE=
=GS2b
-----END PGP PUBLIC KEY BLOCK-----

2.9. Team members

Information on MFA LT CERT members is available upon request.

2.10. Other information

General information about MFA LT CERT can be found at https[:]//www.urm.lt/en
MFA LT CERT Facebook page (mostly in Lithuanian): https[:]//www.facebook.com/urministerija/
MFA LT CERT Twitter profile (mostly in Lithuanian): https[:]//x.com/LithuaniaMFA

2.11. Points of customer contact

The preferred method for contacting MFA LT CERT is via e-mail <CERT_URM (at) urm.lt>. If it is not possible (or not advisable for security reasons) to use e-mail, MFA LT CERT can be reached by telephone during regular office hours. MFA LT CERT 's hours of operation are generally restricted to regular business hours (08:00-17:00 on Monday to Thursday, 08:00-15:45 on Friday except Lithuanian holidays).

3. Charter

3.1. Mission statement

The mission of the MFA LT CERT unit is to ensure the security of the organization’s information systems, data, and digital services by timely identifying, analyzing, and managing cyber threats and incidents, strengthening the institution’s resilience to cyberattacks, and contributing to the continuity of secure and reliable operations.

3.2. Constituency

The MFA LT CERT Security Division provides cybersecurity services to the Ministry of Foreign Affairs of the Republic of Lithuania.

3.3. Sponsorship and/or affiliation

Not available.

3.4. Authority

The main purpose of MFA LT CERT in incident handling is the coordination of incident response.

4. Policies

4.1. Types of incidents and level of support

The CERT LT MFA handles cybersecurity incidents affecting the Ministry of Foreign Affairs of the Republic of Lithuania information systems.
Support is provided exclusively to internal constituents.

4.2. Co-operation, interaction and disclosure of information

- We ensure the protection of confidential information received at the time of the investigation of security incidents and/or prevention of breaches of integrity and unauthorized disclosure of such information, also, that this information is not disclosed, copied or used for any other purposes, which could result in adverse consequences to a person having provided the confidential information, except for cases where obligation is enforced by law.
- CERT LT MFA understands the Traffic Light Protocol (TLP) for sharing sensitive information.

4.3. Communication and authentication

Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data via e-mail, GPG should be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted before or during the transmission.

5. Services

5.1. Incident response

MFA LT CERT Incident Response services are provided to MFA to ensure effective detection, analysis, containment, and resolution of cybersecurity incidents affecting its information systems and operations.

5.1.1. Incident triage
- Determining the extent of the incident. - Investigating whether an incident occurred.
5.1.2. Incident coordination
MFA LT CERT – coordination of cybersecurity incident handling within the organization only.
5.1.3. Incident resolution
Advise local security teams on appropriate actions: - Ask for reports. - Report back. - Collection of evidence after the fact.
5.2. Activities
Available reactive services: - Alerts, warnings, sharing of information. - Incident handling. - Incident analysis. Available proactive services: - Security awareness raising. - Incident coordination. - Education and training.
6. Incident reporting forms
Email: <CERT_URM (at) urm.lt>
7. Disclaimers
While every precaution will be taken in the preparation of information, notifications and alerts, MFA LT CERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.