MFSA MALTA FINANCIAL SERVICES AUTHORITY

# **Significant Cyber Threat**
Notification Process

# CONTENTS

# REVISIONS LOG

| VERSION | DATE ISSUED | DETAILS |
|---|---|---|
| 1.00 | 17 January 2025 | First Release |
| | | |

# Introduction

In line with Chapter III *ICT-related incident management, classification and reporting* of Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (the 'DORA Regulation'), the Malta Financial Services Authority ('MFSA', 'the Authority') is herewith establishing a Significant Cyber Threat Notification process as communicated on 17 January 2025 through Circular titled Cyber Reporting Management System (CRMS).

A Significant Cyber Threat is any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons, with technical characteristics that indicate that it could have the potential to result in a Major ICT-related Incident or a Major Operational or Security Payment-Related Incident.

In establishing this process, the Authority takes into consideration that it applies on a voluntary basis to all Authorised Persons within and/or not in scope of the DORA Regulation. Notification of Significant Cyber Threats is highly encouraged.

The process is being released alongside the following material, which is made available on the MFSA website (Our Work > Supervisory ICT Risk & Cybersecurity):

1. Template for Significant Cyber Threat Notifications ('the Template', 'the provided Template');

2. User Guidelines for submitting Significant Cyber Threat Notifications to the Authority ('the User Guidelines').

# Scope and Applicability

This process and its accompanying material **apply to all Authorised Persons**.

This process applies to **all Authorised Persons within scope of the DORA Regulation** (see Article 2 of the DORA Regulation) **on a voluntary basis** as of 17 January 2025. **All other Authorised Persons not in scope of the DORA Regulation** may also, **on a voluntary basis**, notify Significant Cyber Threats to the Authority, from the date of publication of Circular titled Cyber Reporting Management System (CRMS) and this document, that is, 17 January 2025.

# Definitions

| TERM | DEFINITION |
|---|---|
| Authorised Person | Any person that is licensed, registered or otherwise authorised by the Malta Financial Services Authority. The term 'Licence Holder' is also used by the Authority. |
| Cyber Threat | Any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons [as defined in Article 2, point (8), of Regulation (EU) 2019/881 which is also the definition provided by the DORA Regulation]. |
| DORA Regulation | Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. |
| Major ICT-related Incident | An ICT-related incident that has a high adverse impact on the network and information systems that support critical or important functions of the financial entity [as defined in Article 2, point (13), of the DORA Regulation]. The Authority established a separate process for reporting Major ICT-related Incidents available on the MFSA website. |
| Major Operational or Security Payment-related Incident | An operational or security payment-related incident that has a high adverse impact on the payment-related services provided [as defined in Article 3, point (11), of the DORA Regulation]. The Authority established a separate process for reporting Major Operational or Security Payment-related Incidents available on the MFSA website. |
| MFSA | Malta Financial Services Authority (the 'Authority'). |
| Significant Cyber Threat | A cyber threat the technical characteristics of which indicate that it could have the potential to result in a major ICT-related incident or a major operational or security payment-related incident [as defined in Article 3, point (13), of the DORA Regulation]. |
| SIRC | The Supervisory ICT Risk and Cybersecurity Function within the MFSA. |

# The Notification Process

A Cyber Threat shall be considered as a Significant Cyber Threat where it has met the conditions specified in Chapter III, Article 10 of *Commission Delegated Regulation (EU) 2024/1772 of 13 March 2024, supplementing the DORA Regulation with regard to regulatory technical standards specifying the criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents* (see also *Annex A)*.

Authorised Persons are to notify Significant Cyber Threats to the Authority, on a voluntary basis, through the Cyber Reporting Management System (CRMS) within the License Holder (LH) Portal, using the provided Template.

This process does not replace or supersede any legal obligation by Authorised Persons to notify threats to other competent authorities, unless that legal obligation is specifically superseded by the DORA Regulation.

Authorised Persons may request further information or assistance by calling the SIRC Function on +356 2548 5260 or by sending an email to mirt@mfsa.mt.

# Annex A – Classification of Significant Cyber Threats

In accordance with Chapter III, Article 10 of *Commission Delegated Regulation (EU) 2024/1772 of 13 March 2024, supplementing the DORA Regulation with regard to regulatory technical standards specifying the criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents*, a cyber threat shall be considered significant where all of the following conditions are fulfilled:

(a) the cyber threat, if materialised, could affect or could have affected critical or important functions of the financial entity, or could affect other financial entities, third-party providers, clients or financial counterparts, based on information available to the financial entity;

(b) the cyber threat has a high probability of materialisation at the financial entity or at other financial entities, taking into account at least the following elements:

(i) applicable risks related to the cyber threat referred to in point (a), including potential vulnerabilities of the systems of the financial entity that can be exploited;

(ii) the capabilities and intent of threat actors to the extent known by the financial entity;

(iii) the persistence of the threat and any accrued knowledge about incidents that have impacted the financial entity or its third-party provider, clients or financial counterparts;

(c) the cyber threat could, if materialised, meet any of the following:

(i) the criterion regarding criticality of services set out in Article 18(1), point (e), of the DORA Regulation, as specified in Article 6 of Commission Delegated Regulation (EU) 2024/1772 of 13 March 2024 (criticality of services affected);

(ii) the materiality threshold set out in Article 9(1) of Commission Delegated Regulation (EU) 2024/1772 of 13 March 2024 (clients, financial counterparts and transactions);

(iii) the materiality threshold set out in Article 9(4) of Commission Delegated Regulation (EU) 2024/1772 of 13 March 2024 (geographical spread).

Where, depending on the type of cyber threat and available information, the financial entity concludes that the materiality thresholds set out in Article 9(2) (reputational impact), (3) (duration and service downtime), (5) (data losses) and (6) (economic impact) of *Commission Delegated Regulation (EU) 2024/1772 of 13 March 2024* could be met, those thresholds may also be considered.

Malta Financial Services Authority

Triq L-Imdina, Zone 1

Central Business District, Birkirkara, CBD 1010, Malta

communications@mfsa.mt

www.mfsa.mt