MFSA MALTA FINANCIAL SERVICES AUTHORITY

Circular

05 March 2026

Exercising Caution in Times of Heightened Cyber Threat

The Malta Financial Services Authority (the "Authority") would like to remind Authorised Persons about their obligation to conduct proper situational awareness and regularly assess their exposures to developing ICT and cybersecurity threats, whilst taking timely measures to address them.

The Authority expects Boards of Directors to ensure that ICT and cybersecurity risks are adequately being discussed, that clear roles and responsibilities are set and that ICT and cybersecurity risks are being managed.

Authorised Persons shall, inter alia, review, implement, and enhance the following preventive and detective measures to strengthen their cyber-security posture.

1. Maintain an Elevated Cyber Posture

Continue operating under a higher threat assumption, with increased vigilance across all environments and critical infrastructures.

a. Enforce Multi-Factor Authentication (MFA) for all accounts[1],
b. Enforce least privilege access[2],
c. Prioritise critical and actively exploited vulnerabilities especially front facing systems[3],
d. Maintain continuous monitoring service for logs and alerts[4],
e. Ensure backup resilience and test restore procedures[5]

2. Strengthen Centralised Monitoring and Threat Detection

Ensure continuous visibility of network activity through enhanced coordination, prioritising anomalous authentication events, suspicious traffic patterns, and indicators linked to relevant threat actors.

a. Centralised logs for all critical systems[6],
b. Deploy Advanced Threat Detection technologies[7],
c. Perform threat hunting activities[8]

[1] Reg 2022/2554. Article 9(4)(d)
[2] Reg 2022/2554. Article 9(4)(c)
[3] CDR 2024/1774. Article 10(2)
[4] CDR 2024/1774. Article (12)(2)
[5] Reg 2022/2554. Article 12
[6] CDR 2024/1774. Article 12
[7] CDR 2024/1774. Article 23(2)(a)
[8] CDR 2024/1774. Article 10(2)

3. **Enhance Participation in Information-Sharing Arrangements for Threat Intelligence Sharing**

Authorised Persons are encouraged to participate in trusted Information-Sharing Arrangements to mandate real-time sharing of threat intelligence and ensure immediate awareness of emerging risks.[9]

4. **Ensure Rapid Incident Response Readiness**

Authorised Persons shall re-validate response playbooks, ensuring management and decision makers to receive immediate notification for any confirmed intrusion attempts, coordinated campaigns, or service impacts.[10]

5. **Business Continuity and Switchover Preparedness**

Authorised Persons shall confirm that all critical or important functions are within scope of the ICT business continuity policy.[11]

Finally, transparency and adherence to all relevant guidelines and regulations is critical and essential.

The Authority is gently reminding that, should there have been impact and the ICT-related incident meets the classification criteria for a major ICT-related incident, in line with the Commission Delegated Regulation (EU) 2024/1772, the Authorised Person is to ensure to report it within the stipulated time frames, as per the Commission Delegated Regulation (EU) 2025/301. Further guidance on the reporting process can be referred to here.

Authorised Persons may request further information by sending an email to the Supervisory ICT Risk and Cybersecurity function within the MFSA on mirt@mfsa.mt.

[9] Reg 2022/2554. Article 45
[10] Reg 2022/2554. Article 17
[11] CDR 2024/1774. Chapter IV