INSTRUCTIONS FOR COMPLETING THE CYBERSECURITY INCIDENT REPORTING FORM*

September 2023

*These instructions are reproduced from Appendix II of the Cybersecurity Best Practices Guideline

INSTRUCTIONS

A. Purpose

1. The Central Bank is introducing a **Cybersecurity Incident Report** to facilitate its awareness of, and response to, cyber security incidents at all regulated financial institutions.

2. All companies have a responsibility to address cybersecurity incidents in a timely and effective manner and are required to provide timely notification to the Central Bank when material incidents relating to their operations occur. This requirement should be reflected in the company's policies and procedures for dealing with cyber security incidents.

B. Reportable Incidents

1. Companies should define priority and severity levels within their incident management framework.

2. A reportable incident may have **one or more** of the following characteristics of a material nature:

    a. Impact has potential consequences for other companies or the domestic financial system;

    b. Impacts the company's systems affecting financial market settlement, confirmations or payments (e.g., Financial Market Infrastructure), or impact to payment services;

    c. Impacts operations, infrastructure, data and/or systems, including but not limited to the confidentiality, integrity or availability of customer information;

    d. Disrupts business systems and/or operations, including but not limited to utility or data centre outages or loss or degradation of connectivity;

    e. Causes the disaster recovery teams or plans to be activated or a disaster declaration has been made by a third party vendor that impacts the company;

    f. Impacts a number of external customers and/or negative reputational impact is imminent (e.g., public and/or media disclosure);

    g. An incident assessed by a company to be of high or critical severity, or ranked Priority/Severity/Tier 1 or 2 based on the company's internal assessment; or

    h. Incidents that breach internal risk appetite or thresholds as per the cybersecurity strategy or policy.

3. For incidents that do not align with or contain the specific criteria listed above, or **when a company is uncertain, notification to the Central Bank is encouraged**.

C. Initial Notification Requirements

1. As soon as possible but within **24 hours** of becoming aware of a cyber-incident, the company shall alert the Central Bank, that a cyber-incident has occurred.

2. The company should complete the Cyber Incident Reporting Template below and submit to the Central Bank within **72 hours** of the incident.

3. Where specific details are unavailable at the time of the initial report, the company must indicate 'information not yet available'. In such cases, the company must provide best estimates and all other details available at the time including their expectations of when additional information will be available.

D. Subsequent Reporting Requirements

1. The Central Bank expects the company to provide regular updates (e.g., daily) as new information becomes available, and until all details about the incident have been provided.

2. Until the incident is contained/resolved, the Central Bank expects the company to provide situation updates, including any short term and long-term remediation actions and plans.

3. Following incident containment, recovery and closure, the company should report to the Central Bank on its post-incident review and lessons learnt.

E. Failure to Report

1. Failure to report incidents as outlined above may result in increased supervisory oversight including but not limited to enhanced reporting by the company, and/or the issuance of compliance directions as relevant.