FINANCIAL SERVICES
COMMISSION

Technology and Cyber Risk Management Guideline

POST CONSULTATION PAPER

The Financial Services Commission of Barbados (the "Commission"), as the regulator of non-banking financial services in Barbados, will, from time to time, in accordance with the Financial Services Commission Act, 2010-21issue guidelines that apply to financial institutions which the Commission (the "Commission) regulates. The rationale for the guideline and subsequent consultation paper was circulated to the industry for comments in June 2023.

The period for submitting comments has ended, and the Commission has reviewed the comments received. The attached document includes a summary and the Commission's response to the comments. The guidelines have been finalized, and they, along with the Guideline's Application guide and post-consultation document, will be posted on the Commission's website.

For questions related to the guidelines, kindly submit info@fsc.gov.bb.

1. GENERAL RESPONSES TO SECTION 3 (K) (INCIDENT AND PROBLEM MANAGEMENT)

This section was amended to insert the following:

(1) The occurrence of an IT incident may result in the disruption, malfunction or error on an FI's server, network or end point which can impact its operations and service delivery. FIs should appropriately manage such incidents to understand root cause and appropriate preventative measures to reduce prolonged disruption of IT services or further aggravation.

(2) It is important that incidents are accorded with the appropriate severity level. As part of incident analysis, FIs may delegate the function of determining and assigning incident severity levels to a centralized technical helpdesk function. FIs should train helpdesk staff to discern incidents of high severity level. In addition, criteria used for assessing severity levels of incidents should be established and documented.

(3) *FIs should establish corresponding escalation and resolution procedures where the resolution timeframe is proportionate with the severity level of the incident. The predetermined escalation and response plan for IT security incidents should be tested on a regular basis.*

2. GENERAL RESPONSES TO SECTION 9 (B) (NOTIFICATION REQUIREMENTS)

This section was amended to insert the following:

(1) FIs should inform the FSC within four (4) hours after an incident is classified as major, noting that an incident should be classified within the first twenty-four (24) hours of its detection. An incident is classified as major if it satisfies the requisite criteria in the Classification Matrix found in the Instructions for the completion of the forms.

(2) Cybersecurity events that have a reasonable likelihood of materially harming any part of the normal operation(s) of the FI, should also be reported via the Cyber Incident Reporting Forms to the FSC.

(3) Annually each FI should revise their Cybersecurity program where it has identified areas, systems or processes that require material improvement, updating or redesign. FIs should document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the FSC.

(4) FIs should keep customers informed of any major incident or data breach where their data has potentially been compromised. They should also assess the effectiveness of the mode of communication, including informing the general public, where necessary.

(5) As incidents may stem from numerous factors, FIs should perform a root cause and impact analysis for major incidents which result in disruption of critical IT services. FIs should take remediation actions to prevent the recurrence of similar incidents and security breaches.

(6) FIs should seek further guidance regarding the completion of the forms from Instructions for the completion of the Major Cyber Incident Reporting Forms which is accessible on the FSC's website.

3. GENERAL RESPONSES TO GENERAL COMMENTS

(1) The Glossary of Terms is now placed at the beginning of the guideline after the Purpose and Scope.

(2) All other comments provided are noted and will be considered.