CENTRAL BANK OF BAHRAIN

Appendix -B

Cyber Security Incident Report

Guidance:

1) Section A of the report should be submitted immediately (within one hour) upon occurrence/detection of the cyber security incident.
2) Completed Section B of the report should be submitted within 5 calendar days of the incident occurrence/detection.

Section A: Preliminary Cyber Security Incident Report	
1. Licensee Details	
Date and time of notification to CBB	
Full name of licensee	
Name of official reporting the incident	
• Designation and department	
• Contact details (email, mobile, office telephone)	
Name of official responsible for restoration of the systems and functions	
• Designation and department	
• Contact details (email, mobile, office telephone)	
2. Initial Details of Incident:	
Date and time of incident occurrence and detection	
Who discovered the incident? (*e.g. third-party service provider, customer, employee*)	
Nature of incident and affected areas:	
(a) Outage of IT system (*e.g. back-end systems)*	
(b) Signs of cyber-attack *(e.g. Hacking or malware infection against FI's system, web defacement, distributed denial of service attacks)?*	
(c) Theft or Loss of Information *(e.g. sensitive/important/customer information stolen or missing from business locations)*	
(d) Unavailability of Infrastructure or work premises *(e.g. Power blackout, telecommunication linkages down)*	
(e) Others	
Where are affected systems located (on premises, on cloud etc.)?	
What actions have been taken by the licensee?	
What responses are planned?	

3. Impact (examples are given but not exhaustive):	
(a) Impact on business (*e.g. product offerings, services etc*.)	
(b) Impact on stakeholders (*e.g. affected customers, service providers etc.*)	
(c) Financial and market impact (*e.g. monetary losses etc.)*	
(d) Reputational impact – is the incident likely to attract media attention?	
(e) Regulatory and Legal impact	
(f) Other impacts	

Section B: Comprehensive Cyber Security Incident Report

The comprehensive cyber security incident report should include all information under the following headings:

1. Description of Incident:

(a) Date of incident start time and duration.
(b) Time elapsed from detection to restoration of critical services.
(c) Type of cyber incident (e.g. DDoS, malware, intrusion/unauthorised access, hardware/firmware failure, system software bugs) including if it is a repeat incident.
(d) Impact of the incident (e.g. impact to availability of services, loss of confidential information) including financial, legal and reputational impact and to which group of stakeholders (e.g. retail and corporate customers, settlement institutions, service providers).
(e) Affected systems and technical details of the incident (e.g. source IP address and post, IOCs, tactics, techniques, procedures (TTPs)).
(f) The cyber incident severity level as per below:
- **Severity 1** incident has or will cause a serious disruption or degradation of critical service(s) and there is potentially high impact on public confidence in the licensee.
- **Severity 2** incident has or will cause some degradation of critical services and there is medium impact on public confidence in the licensee.
- **Severity 3** incident has little or no impact to critical services and there is no visible impact on public confidence in the licensee.

2. Root Cause Analysis:

(a) Describe the type of incident (e.g. zero-day attack, exploiting a known vulnerability, isolated incident).
(b) Describe the cause of the cyber incident (e.g. process failure, system failure, human error, external event, malicious action).
(c) Describe whether the cyber incident is due to a third-party service provider.
(d) Describe the attack vector (e.g. malware, virus, worm, malicious hyperlink).
(e) Describe the delivery channel used (e.g. e-mail, web browser, removable storage media).
(f) Describe the impact (e.g. service degradation/disruption, service downtime, potential impact to customers, data leakage, unavailability of data, data destruction/corruption, tarnishing of reputation).
(g) Describe the intent (e.g. malicious, theft, monetary gain, fraud, political, espionage, opportunistic).

(h) Describe the threat actor (e.g. script kiddies, amateur, criminal syndicate, hacktivist, nation state).

3. Response Activities:

(a) List the corrective actions taken:
- Escalation steps;
- Response and recovery activities;
- Stakeholders informed or involved.

(b) Target date of resolution.

(c) Lessons learnt.

(d) Future actions identified to implement preventative measures to ensure similar incidents do not recur.