

OG/134/2022
28th March 2022

Chief Executive Officer
Crypto-Asset Licensees
Manama
Kingdom of Bahrain

Dear Sir/ Madam,

Amendments to Requirements on Reporting Cyber Security Incidents

As part of the Central Bank of Bahrain's (CBB) initiatives to further enhancing its regulatory framework, the CBB is issuing amendments to the requirements under the Crypto-Assets Module (Module CRA) of the CBB Rulebook - Volume 6.

The updated requirements read as follows:

CRA-5.8.19 Upon occurrence or detection of any cyber security incident, whether internal or external, that compromises customer information or disrupts critical services that affect operations, licensees must contact the CBB, immediately (within one hour), on 17547477 and submit the Cyber Security Incident Report (template provided in Appendix 1) to CBB's cyber incident reporting email, incident.cra@cbb.gov.bh, within two hours.

CRA-5.8.19A A licensee, following submission of the preliminary report on detection of a cyber security incident referred to in Paragraph CRA-5.8.19, must submit to the CBB a comprehensive report within **5 10** working days of the occurrence of the cyber security incident. The comprehensive report must include all relevant details including the root cause analysis of the cyber security incident and measures taken by the licensee to ensure that similar events do not recur.

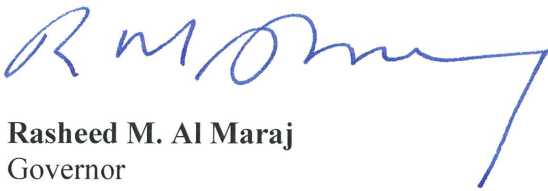


Office of the Governor

The amended requirements are effective immediately and shall be available on the CBB website under the CBB Rulebook - Volume 6 (Ad-hoc Communications) and will also be included as part of the upcoming CBB Rulebook update.

Should you have any queries on this matter, please contact your supervisory point of contact at the CBB.

Yours faithfully,



Rasheed M. Al Maraj
Governor

cc: External Audit Firms