

OG/130/2022
28th March 2022

Chief Executive Officer
All Insurance 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 Risk Management Module (Module RM) of the CBB Rulebook - Volume 3.

The updated requirements read as follows:

RM-9.1.58 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 Section A of the Cyber Security Incident Report (Appendix RM-1) to CBB's cyber incident reporting email, incident.insurance@cbb.gov.bh, within two hours.

RM-9.1.59 Following the submission referred to in Paragraph RM-9.1.58, the licensee must submit to CBB Section B of the Cyber Security Incident Report (Appendix RM-1) within **5 10** calendar days of the occurrence of the cyber security incident. Licensees must include all relevant details in the report, including the full root cause analysis of the cyber security incident, its impact on the business operations and customers, and all measures taken by the licensee to stop the attack, mitigate its impact and to ensure that similar events do not recur. In addition, a weekly progress update must be submitted to CBB until the incident is fully resolved.



Office of the Governor

The amended requirements are effective immediately and shall be available on the CBB website under the CBB Rulebook - Volume 3 (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: Bahrain Insurance Association
cc: External Audit Firms