



EDS/NA/C/03/2025

16<sup>th</sup> July 2025

**Chief Executive Officers**

All Licensees

Manama

Kingdom of Bahrain

Dear Sir/Madam,

**Cyber Security Requirements**

Considering the pivotal role of cybersecurity in safeguarding the stability and operational efficiency of the Kingdom's financial sector, and in line with the Cybersecurity recommendations made by the National Cyber Security Center ("NCSC"), the Central Bank of Bahrain ("CBB") directs all licensees to fully implement the following Cybersecurity measures, with immediate effect:

- a) Ensure public facing systems are kept up-to-date, and any vulnerabilities are promptly addressed.
- b) Enable multi-factor authentication (MFA) protocols for critical systems;
- c) Perform periodic backup of critical systems' data and verify their integrity;
- d) Immediate reporting of any cybersecurity suspicious activity directly on the Cybersecurity Emergency Hotline at 88881 or via email at [CERT@ncsc.gov.bh](mailto:CERT@ncsc.gov.bh).

Licensees are also directed to comply with the recommendations contained in the attached document "Protect Your Organization" based on the nature, complexity and risks of the licensees' systems.

Kindly be advised that these requirements are in addition to the cybersecurity risk provisions outlined in the CBB Rulebook.

Yours faithfully,

**Noora H. Abdulghani**

Executive Director – Supervision

cc: - Bahrain Association of Banks  
- National Cybersecurity Center

Attachment: "Protect Your Organization" issued by NCSC