Date: 17 October 2025

Notice No: FSRA/FCCP/146/2025

To: Senior Executive Officers (SEO) and Principal Representatives (PR) of FSRA's Authorised Persons and Recognised Bodies.

Dear SEO/PR,

RE: Updates to the National Cyber Security Policies from the UAE Cyber Security Council

As part of the Financial & Cyber Crime Prevention Department's (FCCPD) commitment to safeguarding Authorised Persons (APs) and Recognised Bodies (RBs) from emerging cyber threats and strengthening overall cyber resilience, we have been working collaboratively on a national level to remain informed and to further the broader cybersecurity agenda.

A primary focus for the Financial Services Regulatory Authority (FSRA) is to ensure APs and RBs, irrespective of their scale, are equipped with a rigorous cyber risk management framework. Therefore, we would like to draw your attention to newly released and updated polices from the UAE Cyber Security Council (CSC). These policies address critical areas including cyber incident response, information sharing, Security Operations Centre (SOC) baseline capabilities and cloud security. The policies are readily accessible via the following link: https://csc.gov.ae/en/policies-listing

Although adherence to these policies is not mandatory, it is essential for APs and RBs to remain informed about the overarching cybersecurity strategies, policies and best practices adopted nationally.

Particularly, we would like to draw attention to the updated national incident response plan which acts as a useful guide that APs or RBs could use in developing or updating their own incident response plan. This is a requirement under General Rulebook (GEN), specifically section 3.5.16, with an effective date of January 31, 2026.

For any further clarification, APs and RBs are required to reach out by email to fccp-cybercrimeprevention@adgm.com.

Sincerely,

Financial & Cyber Crime Prevention