Frequently Asked Questions: Notice on Cyber Hygiene

Q1. Which are the relevant entities or financial institutions ("FIs") subject to the Notice on Cyber Hygiene? Which Acts will the Notices be issued under?

A1. The FIs to which the Notices apply are:

S/No.	FIs	Act	Notice No
1.	Any insurers and insurance agents	Pursuant to section 29(1) of the Financial Services and Markets Act 2022 (the "Act")	FSM-N04
2.	Any banks		FSM-N06
3.	Any credit card or charge card issuers		FSM-N08
4.	Any finance companies		FSM-N10
5.	All merchant banks		FSM-N12
6.	All licensees, operators and settlement institutions of designated payment systems and digital payment token service providers		FSM-N14
7.	Any designated financial holding companies		FSM-N16
8.	All licensed credit bureaus		FSM-N18
9.	All registered insurance brokers		FSM-N20
10.	All capital markets financial institutions		FSM-N22
11.	Any licensed financial advisers		FSM-N24
12.	Any licensed trust companies		FSM-N26

Q2. In what ways can an FI secure administrative accounts?

A2. Administrative accounts allow users to perform highly sensitive system operations such as starting and stopping system services, modifying critical system settings, assigning system privileges to users and removing system audit trails. System stability and security can be adversely affected if the access to administrative accounts are poorly controlled.

Administrative accounts and access rights should be granted on a "need-to-use" basis. Procedures should be established to assess and approve the granting of administrative accounts. Periodic reviews should be performed to verify that administrative rights are appropriately assigned on a need-to-use basis, and revoked when no longer required.

To safeguard against unauthorised access to administrative accounts, preventive controls such as password complexity, password expiration, dual control of passwords and segregation of duties for system administration, should be implemented.

Q3. What is the appropriate timeframe to apply a security patch? What should the FI do if a security patch is not available to address a known vulnerability?

A3. An FI should adopt a risk-based approach to prioritise the application of security patches. Upon the discovery of a new vulnerability, an FI should assess the severity and develop a remediation plan that is commensurate with (a) the criticality of the affected systems (b) the risks that the vulnerability poses. In this regard, the patching timeframe may differ from one

system to another, or from one vulnerability to another. In the event that a security patch is not available, an FI should take steps to mitigate the risksthat the vulnerability poses. For example, if a zero-day vulnerability has been identified and a patch is not available yet, where applicable, the FI could consider mitigating the risk by using appropriate network security devices to detect and intercept or drop malicious payloads that are targeted to exploit the vulnerability.

Q4. **In relation to the requirements on security standards, can MAS provide examples of security standards contemplated in the notice? What should an FI do if the system cannot conform to the standards?**

A4. FIs can refer to internationally recognised industry best practices from the Center for Internet Security (CIS) and the National Institute of Standards and Technology (NIST) when formulating their security standards. In the event that a system cannot conform to the FI's security standards, the FI should institute appropriate risk mitigating controls and have a process to seek dispensation from its senior management.

Q5. Can MAS prescribe the type of network security devices that FIs can implement to meet the Notice requirement on network perimeter defence?

A5. MAS does not prescribe the types of device that FIs can implement at its network perimeter and to meet the Notice requirement. The types of device to be used would depend on the systems used, the IT operating environment and the associated risks.

Q6. Must an FI implement more than one malware protection measure to meet the Notice requirement?

A6. The implementation of malware protection measures such as anti-virus solution depends on the type of systems to be safeguarded and the IT environment that they operate in. An FI may need to implement measures at the end points, email gateway or internet gateway to mitigate the risk of malware infection.

Q7. Must FIs implement multi-factor authentication for all administrative accounts on critical systems even if the access to these accounts are restricted to internal network?

A7. Passwords can be compromised by an insider or an external intruder who had gained a foothold in the internal network. An FI should implement multi-factor authentication for administrative accounts on its critical systems.

Q8. Must FIs submit an annual attestation or audit report to MAS on their compliance with the Notice?

A8. FIs are not required to submit an attestation or audit report on the compliance with the Notice to MAS. MAS expects an FI to report to its senior management on the state of compliance

with the Notice. MAS will review the extent of FIs' compliance with the Notice requirements as part of our supervisory process.