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.	All merchant banks	This Notice is issued pursuant to section 55(1) as applied by section 55ZJ(1) of the Banking Act (Cap. 19) (the "Act") and applies to all merchant banks in Singapore (each a "relevant entity").	MAS 1118
2.	Any financial holding company	This Notice is issued pursuant to section 28(3) of the Monetary Authority of Singapore Act (Cap. 186) (the "Act") and applies to all financial holding companies ("relevant entity") approved under section 28 of the Act.	MAS 1119
3.	Any bank	This Notice is issued pursuant to section 55(1) of the Banking Act (Cap. 19) (the "Act") and applies to all banks in Singapore ("relevant entity").	MAS 655
4.	Any credit card or charge card issuer	This Notice is issued pursuant to section 57D(1) of the Banking Act (Cap.19) (the "Act") and applies to any person licensed under the Act to carry on the business of issuing credit cards or charge cards, or both in Singapore ("relevant entity").	MAS 655A
5.	Any finance company	This Notice is issued pursuant to section 30(1) of the Finance Companies Act (Cap. 108) (the "Act") and applies to all finance companies ("relevant entity").	MAS 834
6.	Any licensed financial adviser	This Notice is issued pursuant to section 58(1) of the Financial Advisers Act (Cap. 110) (the "Act") and applies to all licensed financial advisers ("relevant entity").	FAA-N21
7.	Any insurer	This Notice is issued pursuant to section 64(2) of the Insurance Act (Cap. 142) (the "Act") and applies to – (a) all licensed insurers; and (b) all insurance agents except for any of the following persons – (c) an individual; and (i) a person exempted from holding a financial adviser's licence under section 23(1)(f) of the Financial Advisers Act (Cap. 110); and (ii) such persons or class of persons as may be exempted from section 6(1) of the Financial Advisers Act (Cap. 110), under	MAS 132

S/No.	FIs	Act	Notice No
		section 100(1) or (2) of the Financial Advisers Act (Cap. 110) (each a "relevant entity").	
8.	All registered insurance brokers	This Notice is issued pursuant to section 64(2) of the Insurance Act (Cap. 142) (the "Act") and applies to all registered insurance brokers (each a "relevant entity").	MAS 507
9.	All licensees and all operators of designated payment systems	This Notice is issued pursuant to section 102(1) of the Payment Services Act 2019 (Act 2 of 2019) (the "Act") and applies to (a) all licensees; and (b) all operators of designated payment systems (each a "relevant entity").	PSN06
10.	Any approved exchange Any recognised market operator Any licensed trade repository Any approved clearing house Any recognised clearing house which are incorporated in Singapore The Depository Any approved holding company Any holder of a capital markets services licence Any registered fund management company Any authorised benchmark administrator, Any authorised benchmark submitter, Any designated benchmark submitter	This Notice is issued pursuant to section 45(1), 46ZK(1), 81R(1), 81SV(1), 81ZL(1), 101(1), 123ZZB(1) and 293(1) of the Securities and Futures Act (Cap. 289) (the "Act") and applies to all - (a) approved exchanges; (b) recognised market operators which are incorporated in Singapore; (c) licensed trade repositories; (d) approved clearing houses; (e) recognised clearing houses which are incorporated in Singapore; (f) the Depository; (g) approved holding companies; (h) holders of a capital markets services licence; (i) Registered Find Management Companies, as defined in regulation 2 of the Securities and Futures (Licensing and Conduct of Business) Regulations; (j) authorised benchmark administrators; (k) authorised benchmark submitters; (l) designated benchmark submitters; and (m) all persons who are approved under section 289 of the Act to act as a trustee of a collective investment scheme which is authorised under section 286 of the Securities and Futures Act and constituted as a unit trust. (each a "relevant entity")	CMG-N03

S/No.	FIs	Act	Notice No
	Any trustee of a collective investment scheme		
11.	Any licensed trust company	This Notice is issued pursuant to section 76(1) of the Trust Companies Act (Cap. 336) (the "Act") and applies to all licensed trust companies ("relevant entity").	TCA-N06
12.	All licensed credit bureaus	This Notice is issued pursuant to section 75(1) of the Credit Bureau Act 2016 (the "Act") and applies to all licensed credit bureaus.	CBN03

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 risks that 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.