# *PwC Straight Away*
# *Public Consultation Paper on MAS Cyber Hygiene Notice*

*13 September 2018*

## Overview of the Cyber Hygiene Consultation Paper

On 6th September 2018, the Monetary Authority of Singapore ("MAS") released a consultation paper on proposed requirements for Financial Institutions ("FIs") in Singapore to implement essential cyber security measures to protect their IT systems. The objective of these requirements is to help FIs strengthen their cyber resilience and guard against cyber-attacks.

The public consultation period will end on 5th October 2018.

This document does not reflect feedback on the consultation paper, but rather an initial point of focus for institutions to assess as they consider internal policies and procedures for adherence to these requirements and/or formal feedback to the MAS.

## 6 Cyber Security Measures

MAS is proposing to stipulate the following six (6) measures as a baseline hygiene standard for cyber security by elevating them into legally binding requirements:

1. **Secure the use of every administrator account** on its system through a combination of preventive controls. These controls include implementing strong password controls, granting access only to authorised staff, keeping a record of all administrative accounts and regularly validating the users having access to administrative accounts.
2. **Address system vulnerabilities in a timely manner** by performing regular checks and applying available security patches. This requires establishing a framework to assess the criticality of system vulnerabilities and stipulating the timeframe within which the patch must be implemented. Mitigating controls must be implemented where no security patch is available.
3. **Establish a written security standard for systems** and ensure **compliance to the security standard**. Mitigating controls should be implemented where the system is unable to conform to the security standard.
4. **Deploy a firewall at its network perimeter** to restrict all unauthorised network traffic and regularly review firewall rules.
5. **Install anti-virus software on its systems** to mitigate the risk of malware infection, and promptly update the (anti-virus) software and signatures.
6. Strengthen user authentication through **implementation of multi-factor authentication** for all administrator accounts on its critical systems, and all accounts on systems used to access confidential information through the internet.

## *Contact us*

If you have any queries, please do not hesitate to call your usual PwC contacts or any of the following PwC subject matter experts:

**Tan Shong Ye**
Digital Trust Leader
*shong.ye.tan@sg.pwc.com*

**Kyra Mattar**
Digital Trust, Financial Services
*kyra.mattar@sg.pwc.com*

**Jimmy Sng**
Digital Trust, Cyber Security
*jimmy.sng@sg.pwc.com*

pwc

## What do FIs need to consider

Whilst the requirements on their own may not be new and are already embedded in good cyber security practices. FIs will need to consider these requirements as legally binding; existing policies and procedures would need to be considered in conjunction with FI's underlying systems and data. FIs should consider:

- System landscape - The extent of the system landscape to which the proposed requirements apply. The requirements proposed over administrator accounts, security patches, security standards and anti-virus apply to ALL systems (i.e. any hardware, software, network, or IT component) used by the entity.

- Critical systems – FIs need to define its critical systems which would require multi-factor authentication for all administrator accounts. Most FIs would have already defined 'critical systems' based on the previous Technology Risk Management Notice.

- Confidential Information – FIs need to determine confidential information applicable to the related entity. **'Confidential information'** is defined as 'any information relating or belonging to the relevant entity that is not publicly available'; this definition is very broad and may include any internal information, such as internal policies and procedures, organisation structure, and even employee portals. FIs will be required to have multi-factor authentication to access 'confidential information' through the internet.

The above are just some of the many areas that FIs need to consider. We would recommend that institutions closely review the consultation paper to identify immediate areas of concerns and assess its pragmatic ability to implement the proposed changes. Additional considerations should be extended to determine the impact on the governance of outsourced services.

## Who is impacted?

The proposed requirements would be applicable to 'relevant entities' that are licensed, approved, registered or regulated by the MAS, including banks, insurers and insurance intermediaries, financial market infrastructures, brokers, financial advisors, fund management companies, finance companies trust companies, credit bureaus, various types of payment services (including money changers, remittance, money transfer, virtual currency, etc) and benchmark administrators.