



Circular No. SRD TR 01/2009

20 March 2009

To Financial Institutions
Chief Executive Officer
Chief Information Officer
Chief Technology Officer
Chief Internal Auditor

Dear Sir / Madam

ENDPOINT SECURITY AND DATA PROTECTION

As financial institutions continue to expand the scope and reach of their online computer systems and customer service call centre operations, they will be confronted with a plethora of data security risks that are becoming more complex, persistent and dynamic. Accordingly, the risk management responsibility of the Board and senior management will increase and intensify commensurately with the scale and complexity of the computer technology, networks, systems, mobile computers and portable storage devices their institutions deploy to provide better customer service and faster access to customer data, financial transactions, account details and other confidential information.

2 Traditionally, security controls for the protection of information assets had been directed mainly at networks, servers, hosts, applications and systems. However, once access to sensitive data has been granted, such controls may not adequately prevent the subsequent loss, leakage or theft of sensitive data from the institutions' endpoint devices such as desktop computers, laptops, mobile phones, portable storage devices and personal digital assistants. In addition, when these mobile or portable devices containing confidential data are taken out of the institutions' work place, the data residing in all these devices may become susceptible to loss, theft or other forms of compromise through mishandling, carelessness, negligence or poor data protection practices.

3 Financial institutions should take appropriate steps to identify the security risks to their information assets, especially customer data processed or stored in endpoint systems as well as those accessible at call centres or other customer service locations. Adequate access controls and security measures should be implemented to detect and prevent unauthorized access, copying or

transmission of confidential data. To enhance the protection of data confidentiality and integrity, customer personal information, identity details and transaction data should be encrypted before they are transmitted, dispatched or delivered to external parties or conveyed on portable storage devices from one location to another.

4 MAS expects all financial institutions to implement appropriate security solutions to address the risk of data theft, data loss and data leakage from endpoint devices, customer service locations and call centres, whether domestic, overseas or under outsourcing arrangements. Confidential customer information stored in all types of endpoint devices should be properly protected with strong encryption. A definitive plan containing specific implementation dates should be formulated to achieve these security targets.

5 Should you have any questions or comments, please contact Mr Tony Chew, Director, Technology Risk Supervision at 62299109 or tonychew@mas.gov.sg.

Yours sincerely

(via MASNET)

CHUA KIM LENG
EXECUTIVE DIRECTOR
SPECIALIST RISK SUPERVISION DEPARTMENT
PRUDENTIAL SUPERVISION GROUP