DIRECTIVE ON THE PARTICIPATING ORGANISATIONS' IT SECURITY STANDARDS AND DISASTER RECOVERY SITE STANDARDS	**No. 5.05-001**

Relevant to	:	Rule 5.05
Introduced with effect from	:	2 May 2013
Amended	:	18 October 2016 vide R/R 7 of 2016
POs' Circular No(s).	:	R/R 9 of 1997 and G 240 of 1999
Refer also to Directive No(s).	:	N/A

1. Rule 5.05

(1) Rule 5.05 requires a Participating Organisation to have:

(a) business premises that are adequately and properly equipped for the conduct of the Participating Organisation's business; and

(b) adequate security and emergency arrangements to provide continuous business operations with minimal disruptions.

(2) In discharging the obligations under the above Rule, a Participating Organisation must, amongst others, comply with the requirements set out below.

(a) the Participating Organisations' IT Security Standards ("PO IT Security Standards") in **Appendix 1** of this Directive; and

(b) the Participating Organisations' Disaster Recovery Site Standards in **Appendix 2** of this Directive.

[End of Directive]

TABLE OF CONTENTS

APPENDIX 1

1.0 GOVERNANCE OF TECHNOLOGY RISKS

OBJECTIVE

The objective of the requirements under Governance of Technology Risks is to ensure that the board of directors and senior management have oversight of technology risks as part of the Participating Organisation ("PO")'s overall framework of managing risk.

1.1 Roles and Responsibilities of Board of Directors

1.1.1 Ensure that the policies and procedures in relation to information technology are established, implemented and communicated to all employees.

1.1.2 Ensure sufficient allocation of resources and security measures to manage cyber security risks, computer systems, networks, data centre, operations and backup facilities.

1.1.3 Ensure that a robust and effective risk management framework to manage technology risk including risk assessment, monitoring and reporting is established.

1.1.4 Ensure sufficient and continuous awareness and education programmes are provided to all employees.

1.2 Technology Risk Management

1.2.1 A robust technology risk management framework should be established and be reviewed on a periodical basis. It may include the risk identification, risk assessment, risk mitigation, risk monitoring and reporting.

1.2.2 Sufficient and proper risk identification policies, procedures and processes to determine relevant security threats and vulnerabilities should be established and may include scenarios such as denial of service attack, internal sabotage and malware infestation which can harm and disrupt the organisation's operations.

1.2.3 Relevant and sufficient risk mitigation measures should be in place to mitigate the identified risk to minimise the risk exposure to the organisation.

1.3 Information Security Policies

1.3.1 Policies for information security including cybersecurity must be defined and set out the organisation approach to achieving its information security objectives.

1.3.2 The information security policy must be approved by the Board of Directors and communicated to all employees.

1.3.3 Information security policies should contain the following statements:

a) definition, objectives and principles to guide all activities relating to the information security of all relevant activities;

b) defined roles, responsibilities and accountabilities of key personnel to manage information security risks, including that of a chief information security officer, chief technology officer, head of business unit and risk management; and

c) processes for handling deviation and exceptions.

1.3.4 Information security policies must be regularly reviewed for continuing suitability, adequacy and effectiveness.

1.3.5 The information security policies should be assessed in response to changes to the organizational environment, business circumstances and regulatory requirements.

2.0 ORGANISATION OF INFORMATION SECURITY

OBJECTIVE

The objective of the requirements under Organisation of Information Security is to ensure that a management framework is established to initiate and control the implementation and operation of information security within the PO.

2.1 Internal Organisation

2.1.1 Responsibilities for the management and administration of information technology security must be defined and assigned to the relevant personnel.

2.1.2 For each application system, the following must be identified:

a) **Data Owners**

Responsible for business data captured, stored and processed by information systems.

b) **System Owners**

Responsible for business systems and approving changes to the applications. Owners of the system software must be similarly responsible for approving change in their area.

c) **System Users**

Any persons using the information processing facilities in the course of their normal duties and responsible to ensure that the information processing facilities are used only for authorised purposes.

d) **System Providers**

Functional groups who are responsible for providing information systems to System Owners and System Users.

e) **Procedure Owners**

Managers who are responsible for ensuring that the procedures supporting the business process are up-to-date.

2.2 Information Security Responsibilities

2.2.1 All information security responsibilities must be defined, allocated and approved by the IT Management.

a) **Security Administration Responsibilities**

i. The assignment of the Security Administration roles and responsibilities must be clearly set out and documented.

ii. Persons responsible for Security Administration must be appointed with responsibility for:

(1) administration of access controls software;

(2) reviewing access rights on a regular basis to ensure compliance with these Standards; and

(3) monitoring and investigating security violation attempts.

b) **Data Owner Responsibilities**

Data Owners must:

i. in conjunction with Security Administration, ensure that the controls over user access have been defined and documented;

ii. authorise users' access and their required access rights to the data;

iii. authorise amendments made to sensitive data; and

iv. review access profiles at least once a year.

c) **System Owner Responsibilities**

i. System Owners must:

(1) specify the processes for each business function. Where a process uses information processing facilities, the functional requirements of an application and the manual procedures should be defined and agreed;

(2) verify that the systems meet with users' requirements;

(3) ensure that the controls required within the process are defined and agreed; and

(4) authorise users to use system functions. When authorising access, the System Owner must consider the following to ensure the allocation of appropriate access rights:

- compatibility with other responsibilities and existing access rights of the user
- the classification of the information
- whether the requested level of access is required in order to allow the user to carry out in accordance to his/her job function

ii. The System Owner and Data Owner may be the same individual.

iii. The System Owner and Data Owner must ensure that regular checks which include penetration testing for compliance with security requirements for all information processing facilities are carried out.

d) **System User Responsibilities**

System Users must:

i. ensure the confidentiality of their user IDs and passwords; and

ii. ensure that the information processing facilities are used only for authorised purposes to protect the information processing equipment placed in their care.

e) **System Provider Responsibilities**

System Providers must:

i. provide defined and agreed levels of security for computing facilities;

ii. ensure that application systems are free from interference by other systems; and

iii. administer any specified controls that have been defined and agreed.

f) **Procedure Owner Responsibilities**

Procedure Owners must:

i. provide documented procedures to the users of the system;

ii. ensure that the procedures for all the systems are up-to-date; and

iii. ensure that the procedures conform to the PO IT Security Standards.

2.3 Segregation of Duties

2.3.1 Where the performance of the duties and areas of responsibility by the same person could give rise to conflicts of interests, such duties and areas of responsibility must be segregated. Hence, the following duties should be segregated based on the size and complexity of the business:

a) application development;

b) technical support;

c) computer operations;

d) quality assurance;

e) internal audit;

f) security administration; and

g) user departments.

3.0 HUMAN RESOURCE SECURITY

OBJECTIVE

The objective of the requirements under Human Resource Security is to ensure that employees understand their roles and responsibilities and are suitable for the roles to which they have been assigned, to minimize the risks of theft, fraud or misuse of POs' information processing facilities.

3.1 Prior to Employment

3.1.1 Pre-Employment - Screening

a) Background verification checks on all candidates for employment must be carried out and should include an investigation into a candidate's career history and the verification of academic and professional qualifications.

b) New employees must be placed on probationary status for IT functions and their progress be reviewed to ensure that they are performing their duties adequately.

3.1.2 Terms and Conditions of Employment

a) All employees must sign a contract of employment that establishes their duties with respect to information technology security.

b) The contract of employment or other relevant documents must include the following arrangements for all employees:

i. a confidentiality undertaking relating to disclosure of information;

ii. the requirement to report any observed or suspected security weaknesses;

iii. the intellectual property rights over any designs, procedures or inventions made, created or designed by the employee; and

iv. the disciplinary procedures that will apply for employees found to have violated the PO IT Security Standards.

3.2 During Employment

3.2.1 Management Responsibilities

a) All employees must be briefed on their information security roles and responsibilities prior to being granted access to confidential information or information systems.

b) The Management must ensure all employees conform to the terms and conditions of employment, which include the PO IT Security Standards.

3.2.2 Roles and Responsibilities

a) Detailed employee's roles and responsibilities (including IT security responsibilities) must be documented and communicated to the individual employee.

b) Roles and responsibilities must be acknowledged by the employee.

3.2.3 Training On Information Security Awareness

a) Information security training must be provided to all new employees and reinforced on an on-going basis to create and maintain awareness among the employees.

b) An information security awareness programme should be established in line with the organisation's information security policies and relevant procedures and updated regularly.

c) Reinforcement of information security training should be given to all employees on periodic basis.

3.2.4 Disciplinary Procedures

a) A formal disciplinary process must be established to take action against employees who have committed the information security breach.

3.3 Termination and Change of Employment

3.3.1 Termination or Change of Employment Responsibilities

a) There must be a policy established to ensure that prompt notification of all employees' resignations/movements is made by relevant departments to Security Administration and prompt action is taken to revoke or amend access rights.

4.0 ASSET MANAGEMENT

OBJECTIVE

The objective of the requirements under Asset Management is to ensure a PO's assets are appropriately defined and are adequately protected from unauthorised access.

4.1 Inventory of Assets

4.1.1 POs must maintain an inventory of assets associated with information and information processing facilities.

4.1.2 The inventory listings must be accurate, up to date, consistent and aligned with other inventories.

4.1.3 POs must identify the owner for all assets.

4.1.4 The owner of the assets should be responsible for the following:-

a) Define the classification of the information and the assets associated with information processing;

b) Review the classification level and keep it up to date; and

c) Ensure proper handling of the asset when the asset is deleted or destroyed.

4.2 Information Classification

4.2.1 POs may classify the assets based on legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.

4.2.2 POs may consider the business needs and impacts when defining the classification and protective controls for the information and such classification and protective controls should include the confidentiality, integrity and availability of the information.

4.2.3 POs may establish an Information Classification Policy for the entire organisation.

4.2.4 POs may classify the assets as follows:-

a) Restricted

b) Confidential

c) Public

4.2.5 POs may establish procedures for information labelling in accordance to the Information Classification Policy adopted by the POs.

4.2.6 POs may use other means of classification of information if labelling is not feasible and such other means of classification must be approved by the owner.

5.0 ACCESS CONTROL

OBJECTIVE

The objective of the requirements under Access Control is to restrict access to information and information processing facilities to authorised users.

5.1 Logical Access Policy

5.1.1 Logical Access Policy must be established, documented and approved by the Data Owner based on the following:

a) business and information security requirements;

b) the organization and departmental policies for information dissemination and entitlement; and

c) contractual obligations and legal requirements regarding the limitation of access to data or services.

5.1.2 The Logical Access Policy must include the access to the critical application system, operating system and network services.

5.1.3 The Logical Access Policy must be used to enforce the segregation of duties between incompatible job functions.

5.2 User Access Administration

5.2.1 The Logical Access Policy for the creation, amendment and maintenance of user ID and user profiles must be defined, agreed and documented.

5.2.2 The Logical Access Policy must take into account the following:

a) controlling what data can be accessed by a particular user; and

b) controlling the access rights of users, e.g. read, write, delete and execute.

5.2.3 The requests for user access to the application function, operating system and network resources must be granted on the basis of written requests authorised by the Data Owner.

5.2.4 Remote access to third party service providers/vendors may only be granted upon approval by the Data Owner. All remote access must be under the control of Security Administration and the remote users' activities must be logged and monitored by the Security Administration.

5.2.5 POs must establish a policy on revoking access rights granted to user, taking into the consideration the following:-

a) Users who have changed roles or jobs;

b) Users who have left the organisation; and

c) Termination of contract for external third party users.

5.3 User Authentication Management

5.3.1 Each user must be required to identify himself or herself to the system with a recognised approved user ID and a secret authentication (password) to authenticate his/her identity.

5.3.2 Procedures must be established to verify the identity of a user prior to providing new, replacement or temporary secret authentication information.

5.3.3 Secret authentication must be unique to an individual and must not be easily guessable.

5.3.4 Users must change their secret authentication at first log on.

5.3.5 Users must not divulge their secret authentication.

5.3.6 Users must not share their user ID.

5.3.7 POs must establish a policy for the usage of shared user ID where sharing is necessary for business or operational reasons.

5.3.8 All default user ID must be disabled.

5.3.9 POs must establish a policy on secret authentication when passwords are used as secret authentication. The password management system must include the following minimum requirements:

a) The system must allow case sensitive password;

b) The system must allow Administrator to change and set expiry of the password;

c) The system must force users to change their passwords at the first log-on;

d) The system must maintain a history of user passwords and prevent reuse of recent or similar passwords; and

e) Cryptography techniques must be used to authenticate the authorised access if access is done through public network for all critical transactions such as fund transfers, securities transfer or high value trading transactions.

5.4 Management of Privileged IDs

5.4.1 The privileged IDs must be restricted, controlled and granted upon the approval by the Data Owner in accordance to the Logical Access Policy.

5.4.2 The privileged access rights associated with each system i.e. operating system, database management system and each application must be identified.

5.4.3 The privileged IDs assigned to a user must be different from those used for normal operation functions.

5.5 Review of User Access Rights

5.5.1 POs must establish a policy to ensure the access to all information system be reviewed to ensure all access granted is restricted to authorised personnel only. The policy must include review of the following areas:

a) unauthorised access attempts;

b) maintenance to security profiles or security tables;

c) use of sensitive commands;

d) privileged user’s activity;

e) access by third party vendors / engineers; and

f) identifying redundant user IDs.

5.5.2 The User Access Profile must be reviewed on a regular basis by the relevant authorised personnel. At a minimum, the review must be undertaken at least once a year.

5.6 Secure Log on Procedures

5.6.1 The access to operating systems and applications must be controlled by a secure log-on procedure.

5.6.2 A good log on procedure should have the following features:-

a) does not display system or applicant identifiers until the log-on process has been successfully completed;

b) validates the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect;

c) displays previous successful log-on upon completion of successful log-on; and

d) provides details of any unsuccessful log-on attempts since the last successful log-on.

PHYSICAL AND ENVIRONMENTAL SECURITY

6.0 PHYSICAL AND ENVIRONMENTAL SECURITY

OBJECTIVE

The objective of the requirements under Physical and Environmental Controls is to prevent unauthorised physical access, damage and interference to the PO's information and information processing facilities.

6.1 Secure Area

6.1.1 Secure locations of sensitive areas must be identified and documented as part of the physical access control procedures.

6.1.2 Security perimeters must be defined and used to protect areas that contain sensitive and critical information. A manned reception area or other means of physical access control must be in place to ensure access is restricted to authorised personnel only.

6.1.3 Appropriate physical entry controls to offices, rooms and facilities should be established and access by visitors and non-authorised personnel to secure locations must be authorised, logged and supervised by an authorised personnel.

6.1.4 The access rights to secure locations and sensitive areas must be regularly reviewed and updated.

6.1.5 Physical protection against natural disaster, malicious attack or accidents should be designed and applied.

6.2 Equipment

6.2.1 Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.

6.2.2 Critical computer related equipment and information system must be protected by an automatic fire detection and alarm system. Installation of fire suppression systems must comply with local regulations.

6.2.3 Equipment must be protected from power failures and other disruptions caused by failures in supporting utilities. Power supplies to critical system must be protected and backup sources must be available to ensure continuity of processing.

6.2.4 Supporting utilities must conform to equipment manufacturer's specification and be subject to regular inspection.

6.2.5 Equipment should not be taken off-site without prior authorisation. Movement of the assets should be recorded accordingly.

6.3 Storage Media

6.3.1 Access to computerised storage media must be restricted only to authorised personnel and adequately protected from physical and environmental damage.

6.3.2 All movement of computerised storage media to and from storage must be logged accordingly.

6.3.3 All items of equipment containing storage media must be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

6.4 Secure disposal or re-use of equipment

6.4.1 Authority to dispose the equipment containing storage media must be granted to authorised personnel.

6.4.2 The equipment containing storage must be destroyed, deleted or overwritten using techniques that ensure the original information is non-retrievable before disposal.

6.4.3 Records for the disposed equipment should be maintained.

6.5 Emergency Procedures

6.5.1 Emergency and evacuation procedures must be documented and made available to all personnel.

6.5.2 The emergency procedures must be tested at least once a year.

6.5.3 Personnel must be adequately trained to handle emergencies.

7.0 OPERATIONS SECURITY

OBJECTIVE

The objective of the requirements under Operations Security is to ensure the correct and secure operation of the information processing facilities.

7.1 Documented Operational Procedures

7.1.1 POs must establish and document procedures for operational activities associated with information processing and communication facilities such as computer start-up and close-down, backups, media handling, equipment maintenance, and computer room.

7.1.2 The operating procedures should specify the operational instructions, including:

a) the installation and configuration of systems;

b) processing and handling of information both automated and manual;

c) backup;

d) scheduling requirements such as job starts and day end job;

e) instructions for handling errors or other exceptional conditions, which might arise during job execution;

f) support and escalation contacts including third party support;

g) media handling instructions;

h) system restart and recovery procedures; and

i) management of audit-trail and system log information.

7.1.3 All documentation in relation to Operations Security must be maintained and regularly updated to ensure information is up-to-date, complete and accurate. The changes must be reviewed and approved by the Management.

7.2 Change Management

7.2.1 All changes to the systems and information processing must be documented, assessed on the potential impacts, approved and tested prior to its implementation.

7.2.2 In particular, the following items should be considered:

a) identification and recording of significant changes;

b) planning and testing of changes;

c) assessment of the potential impacts, including security impacts;

d) formal approval procedure for proposed changes;

e) verification that information security requirements have been met;

f) communication of change details to all relevant parties;

g) fall-back procedures including procedures for recovering from unsuccessful changes and unforeseen events; and

h) provision of an emergency change process.

7.2.3 All changes made must be logged and the audit log containing all relevant information must be retained.

7.3 Capacity Management

7.3.1 POs must monitor and plan future capacity requirements for hardware, software and network to ensure the required performance is retained.

7.3.2 The business criticality of the concerned system should be taken into account in any capacity planning.

7.3.3 Capacity management plan should be established for mission critical systems.

7.3.4 Capacity planning must be performed and reviewed on a regular basis, at least once a year.

7.4 Segregation of Logical System Environments

7.4.1 The following logical system environments should be established to mitigate the risks of accidental change and unauthorised access to operational software and business data:

a) Development;

b) Test; and

c) Production.

7.4.2 POs must segregate the following duties within the IT activities:

a) Computer Operations;

b) Technical Support; and

c) Application Development.

7.4.3 End users must be restricted to business application functions and must not have access to systems software and utilities.

7.4.4 The testing environment should be consistent with the production environment to ensure adequate levels of confidence in the testing.

7.5 Handling of Information Backup

7.5.1 All backup media must be recorded, uniquely identified, stored securely and subjected to secure disposal procedures.

7.5.2 Backups should be protected by means of encryption where confidentiality is of importance.

7.5.3 All storage media must be uniquely labelled to identify the contents.

7.5.4 Centralised inventory listings of all storage media must be maintained for both on-site and off-site locations.

7.5.5 The retention period of backups must be defined and agreed by System Owners and Data Owners in accordance with relevant regulatory requirements, taking into account any requirement for archive copies to be permanently retained.

7.5.6 If a third party has been authorised to store backup media, a Supplier Agreement must be defined and documented, and in compliance with the PO IT Security Standards.

7.6 Security over Computer Reports

7.6.1 Access to confidential output and printers generating confidential information must be restricted only to authorised personnel.

7.6.2 Documents containing confidential information must be rendered unreadable prior to disposal.

7.7 Logging and Monitoring

7.7.1 Event logs, including the operator console activity, where applicable, must be maintained as an audit trail and reviewed.

7.7.2 Details of event logs should include the following, where relevant but which is not exhaustive:

a) User IDs;

b) System activities;

c) Dates, times and details of key events;

d) Device identity or location and system identifier;

e) Records of successful and rejected system access attempts;

f) Changes to system configuration;

g) Use of privileges;

h) Use of system utilities and applications;

i) Files accessed and the details of access;

j) Network addresses and protocols;

k) Alarm raised by the access control system;

l) Activation and de-activation of protection systems e.g. anti-virus systems and intrusion detection systems; and

m) Records of transaction executed by users in applications.

7.7.3 The event log:

a) must be archived until all outstanding problems which require reference to it have been resolved, after which it may be purged;

b) must be archived for a minimum period of at least one year; and

c) must be audited.

7.7.4 System exceptions must be identified, highlighted and monitored by Computer Operations personnel or other personnel designated to respond to such exception conditions.

7.7.5 Controls must be in place to ensure the following:

a) No alterations are made to the recorded message types;

b) Log files are not edited or deleted; and

c) No failure in recording the events or over-writing past recorded events in the event the storage of the log file media has exceeded its storage capacity.

7.7.6 System administrators must not have permission to erase or de-activate logs of their own activities.

7.7.7 Computer operations personnel must not be able to bypass the logging process and update or delete entries from the system log.

7.7.8 The correct setting of computer clock is important to ensure accuracy of audit logs. A network time protocol can be used to keep all servers in synchronisation with master clock.

7.7.9 Powerful utility programs capable of bypassing logical access controls must be:

a) Stored in secured libraries;

b) Restricted to a minimum number of authorised users; and

c) Protected from being copied or renamed.

7.7.10 Access to powerful utilities must be authorised. The use of powerful utilities must be monitored and logged by Security Administration.

7.7.11 All unauthorised access attempts and other security related events must be logged and should be subjected to review by Security Administration.

7.7.12 Where systems permit, violation report must be produced for review by Security Administration on a daily basis.

7.7.13 All unauthorised access attempts and other security violations reported must be investigated by Security Administration.

7.8 Protection from Malware

7.8.1 Controls should be in place to ensure information and processing facilities are protected against malware.

7.8.2 POs must put in place the following controls:

a) Establishing a formal policy prohibiting the use of unauthorised software;

b) Implementing controls that prevent or detect the use of unauthorised software;

c) Implementing controls that prevent or detect the use of known or suspicious malicious websites;

d) Establishing a formal policy to protect against risks associated with obtaining files and software either from or via external networks or on any other medium;

e) Defining procedures to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks;

f) Implementing procedures to verify information relating to malware to ensure warning bulletins are accurate and informative, and all users should be made aware of the problem of hoaxes;

g) Regular reviews of the software and data content of systems supporting critical business processes must be conducted and the presence of any unapproved files or unauthorised amendments must be formally investigated;

h) Installing and regularly updating of malware detection software ; and

i) Business continuity plans must include recovering from malware attacks and any other cyber threats covering all necessary data and software backup and recovery arrangements, and isolating environments when there is catastrophic impacts.

8.0 NETWORK AND COMMUNICATION SECURITY

OBJECTIVE

The objective of the requirements under Network and Communication Security is to ensure information in networks and its supporting information processing facilities are adequately protected from unauthorised access.

8.1 Network Controls

8.1.1 POs must establish the responsibilities and procedures for the management of networking equipment.

8.1.2 POs must establish controls to safeguard the confidentiality and integrity of data that are transmitting over public networks or wireless networks.

8.1.3 POs must establish controls to ensure the availability of the networks and services connected.

8.1.4 POs must ensure appropriate logging and monitoring controls are established to enable recording and detection of actions that may affect the information security.

8.1.5 POs should ensure controls are in place to identify equipment or systems that can be connected to the POs' private network.

8.1.6 POs must establish adequate controls if the use of dial-back are allowed. POs are advised to test the dial back procedures to prevent unauthorised and unwanted connection to POs' private network.

8.1.7 POs must ensure all changes to the network configuration require authorisation.

8.1.8 POs must maintain a list of network users and systems communicating via the network.

8.1.9 POs should disable all network services and facilities when not in use.

8.2 Segregation of Networks

8.2.1 POs must segregate the group of information services, users and information based on different network domain in accordance to the POs' access control policy.

8.2.2 POs may consider segregation based on the following domain:

a) Internal network domains;

b) External network domains; and

c) Wireless network domains.

8.2.3 The network segregation should be based on the value and classification of the information stored or processed in the network.

8.3 Network Security

8.3.1 Procedures to control the flow of information and access control between the internal and external network should be established.

8.3.2 POs must define the perimeter and firewalls must be used to protect and segregate the internal network, external networks and wireless network.

8.3.3 Cryptographic method and strong authentication should be considered for wireless network implementation.

8.3.4 Network diagrams must be maintained and any changes must be updated.

8.3.5 Access to network port for remote diagnostic activity and configuration must be approved by the System Owner.

8.3.6 POs should use cryptographic techniques to protect the confidentiality, integrity and authenticity of information transmitted through mobile or removable media, devices or across communication lines.

8.3.7 POs must establish policies to perform vulnerability assessment and penetration testing on its network or internet based application system.

8.3.8 All network management software should at least include the following features:

a) Monitoring of users' activity and attempted security violations; and

b) Monitoring capabilities to track and report network status or network error.

8.3.9 Procedures must be developed to minimize the risk of viruses causing damage to data and program.

8.3.10 All critical servers and workstations must be installed with anti-virus software.

8.3.11 All anti-virus software must be auto-executed upon login to the local area network and upon PC start-up.

9.0 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

OBJECTIVE

The objective of the requirements under System Acquisition, Development and Maintenance is to ensure that information security is an integral part of information systems across the entire systems life cycle.

9.1 Security Requirements of Information Systems

9.1.1 POs must ensure that the following information security related requirements be included for new information system or enhancements to the existing system:

a) access provisioning and authorisation processes, for business users as well as for privileged or technical users;

b) the required protection needs of the assets involved, in particular regarding availability, confidentiality and integrity;

c) requirements derived from business processes, such as transaction logging and monitoring; and

d) requirements on other security controls, e.g. interfaces to logging and monitoring or data.

9.1.2 POs must ensure that security requirements and controls reflect the business value of the information assets and the potential business impact resulting from lack of adequate security.

9.1.3 POs must integrate security requirements and the processes for implementing security in the early stages of information system projects.

9.1.4 POs must ensure that a formal testing process is completed for any product before an acquisition or procurement.

9.1.5 Any contracts with the vendor should address the security requirements.

9.2 Access Control to Source Code

9.2.1 POs must ensure that access control to program source code be restricted and controlled, in order to prevent unauthorised functionality and to avoid unintentional changes as well as to maintain the confidentiality of valuable intellectual property.

9.2.2 For program source code, this can be achieved by having a controlled central storage of such code, preferably in program source libraries. The following guidelines may be considered to control access to such program source libraries:

a) program source libraries should not be held in production environment;

b) the program source code and the program source libraries should be managed according to established procedures;

c) the updating of program source libraries associated items and the issuing of program sources to programmers should only be performed after appropriate authorisation has been received;

d) an audit log must be maintained of all accesses to program source libraries; and

e) maintenance and copying of program source libraries must be subject to strict change control procedures.

9.3 Security in Development and Support Process

9.3.1 Secure Development Policy

a) POs must ensure the policy on the development of software and systems be established and the following should be considered:-

i. security of the development environment;

ii. guidance on the security in the software development lifecycle;

iii. security in the software development methodology;

iv. secure coding guidelines for each programming language used;

v. security requirements in the design phase;

vi. security checkpoints within the project milestones; and

vii. security in the version control.

9.4 System Change Control Procedures

9.4.1 POs must ensure the changes for new systems and major changes to the existing system within the development lifecycle are subjected to formal change control procedures.

9.4.2 The change control procedures must include the following:

a) changes must be via formal written instructions by authorised users;

b) controls and integrity procedures must be subject to review to ensure that they will not be compromised by the changes;

c) all software, information, database entities and hardware that require amendment must be identified;

d) formal approval for detailed proposals must be obtained before work commences;

e) changes are subject to acceptance by the users prior to implementation;

f) the system documentation is updated on the completion of each change and that old documentation is archived or disposed of;

g) a version control for all software updates is maintained;

h) an audit trail of all change requests is required;

i) that operating documentation and user procedures are approved prior to any changes; and

j) the implementation of changes takes place at the appropriate time and does not disturb the business processes involved.

9.5 Restrictions on changes to software packages

9.5.1 When a vendor supplied software package needs to be modified, POs must ensure that the processes comply with the established change or modification policies and procedures.

9.5.2 POs must ensure that if changes are necessary, the original software is retained and the changes applied to a designated copy.

9.5.3 POs must ensure that the software update management process is implemented with the most up-to-date approved patches and application updates are installed for all authorised software.

9.5.4 POs must ensure that all changes and modification are fully tested, validated by an independent party and documented, so that they can be reapplied, if necessary, to future software upgrades.

9.6 System Security Testing Control

9.6.1 POs must ensure the testing of security functionality is carried out during the development phase.

9.6.2 POs must require thorough testing and verification during the development processes.

9.6.3 For in-house developments, tests must initially be performed by the development team. Independent acceptance testing must be undertaken to ensure that the system works as expected.

9.7 System Acceptance Testing Control

9.7.1 POs must establish acceptance testing programs and related criteria for new information systems, upgrades and new versions of software.

9.7.2 System acceptance testing must also include testing of information security requirements.

9.7.3 Testing should be performed thoroughly to ensure that the system will not introduce vulnerabilities to the PO's environment and that the tests are reliable.

9.8 **Test data**

9.8.1 POs must ensure the following guidelines are applied to protect operational data, when used for testing purposes:

a) authorisation is required each time when operational information is copied to a test environment;

b) data masking and massaging must be carried out for sensitive information;

c) operational information should be erased from a test environment immediately after the testing is complete; and

d) copying and use of operational information should be logged to provide an audit trail.

10.0 SUPPLIER MANAGEMENT

OBJECTIVE

The objective of the requirements under Supplier Management is to ensure that the information access granted to a supplier is adequately protected.

10.1 Information Security in Supplier Management

10.1.1 POs must establish a policy to address the information security risks for its outsourcing activities such as data centre operations, network administration, disaster recovery site, application hosting and cloud computing. POs may consider the following areas:

a) Identify the types of suppliers whom a PO will allow to access its information;

b) Define types of allowable information access for different types of suppliers and procedures on monitoring and controlling the access;

c) Put controls in place to ensure the integrity of the information processing provided by the suppliers; and

d) Put in place recovery and contingency arrangements to ensure the availability of information processing by the suppliers within the required recovery time objective ("RTO").

10.2 Engagement of Suppliers

10.2.1 Background verification checks on all suppliers must be carried out and suppliers engaged to handle sensitive information must be subjected to adequate investigation and review before being engaged.

10.2.2 Work undertaken by supplier's service providers must be subject to compliance with the PO IT Security Standards.

10.2.3 Suppliers must sign a statement of confidentiality.

10.3 Suppliers Agreements

10.3.1 POs must establish the suppliers' agreement to document both parties' obligations in fulfilling relevant security requirements.

10.3.2 POs may include the following terms in the suppliers' agreements:

a) legal and regulatory obligations, including data protection and intellectual property rights;

b) an agreed set of controls of each contractual party to be implemented including access control, performance review, monitoring, reporting and auditing;

c) incident management requirements and procedures;

d) contractual rights to audit the supplier's process;

e) escrow arrangement for outsourced software development;

f) provisions of evidence that sufficient testing has been applied to guard against the malicious content upon delivery known vulnerabilities; and

g) suppliers' obligations to comply with the PO's security requirements.

10.4 Management of Suppliers Service Delivery

10.4.1 POs must regularly monitor service performance levels of the supplier to verify adherence to the terms defined in the suppliers' agreements.

10.4.2 POs must review service reports produced by the supplier.

10.4.3 POs must ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster.

11.0 INFORMATION SECURITY INCIDENT MANAGEMENT

OBJECTIVE

The objective of the requirements under the Information Security Incident Management is to ensure that the information security incidents and communication on security events are managed effectively.

11.1 Responsibilities and Procedures

11.1.1 POs must establish the following procedures to ensure effective and orderly response to information security incidents:

a) Procedures for monitoring, detecting, analysing and reporting of information security events and incidents;

b) Procedures for logging incidents;

c) Procedures for incident response planning and preparation; and

d) Procedures for escalation and recovery from an incident and communication to internal and external parties.

11.1.2 POs should integrate the information security incident response plan with the Business Continuity Plan.

11.2 Reporting Information Security Events

11.2.1 POs must ensure that all its employees and contractors are made aware of their responsibility to report any information security events. Information security events may include the following:

a) Ineffective security controls;

b) Breach of information integrity, confidentiality or availability expectations i.e. denial of service;

c) Human errors;

d) Non-compliances with policies and procedures or guidelines;

e) Breaches of physical security arrangements;

f) Malfunctions of software or hardware;

g) Access violations; and

h) Misuse or abuse of facilities.

11.3 Incident Logging

11.3.1 All incidents reported must be formally logged in a consistent format in a central location.

11.3.2 POs must ensure that access to the incident log is restricted to authorised personnel.

11.3.3 POs must include the following details in the incident log:

a) the date and time the incident was logged;

b) a summary description of the nature of the incident ;

c) how the incident was identified;

d) who reported the incident (i.e. name / department / designation);

e) the extent of the incident and its implications on other components of the system;

f) the priority of the incident ; and

g) details of all diagnostic or attempted recovery actions taken.

11.3.4 The priority of the incident must be determined with consideration given to the nature of the incident, its impact on data confidentiality, integrity and availability, and the business functions to which the incident relates.

11.4 Incident Investigation and Diagnosis

11.4.1 All logged incidents must be promptly assigned to the appropriate personnel for investigation, diagnosis and correction.

11.4.2 The incident assignee should conduct an impact analysis and diagnosis of the potential cause of the problem before taking action to resolve the incident. A summary of the analysis, diagnosis, and proposed action to be taken to resolve the incident should be documented.

11.4.3 The incident assignee must ensure that each logged incident has been correctly classified in respect of priority before workaround or taking any action.

11.4.4 If the incident assignee cannot diagnose the cause or find a suitable solution, the incident should be escalated to the Management.

11.5 **Incident Resolving and Recovery**

11.5.1 All incidents must be resolved and recovered on a timely basis according to their priority and agreed dates and time of resolution.

11.5.2 An investigation should be conducted on the root cause of all logged incidents to determine the recognised incident solving techniques that can be used to help in resolving and recovery.

11.5.3 The action taken to resolve the logged incident must be documented with appropriate details to enable an independent person to analyse the actions taken without recourse to the incident assignee.

11.6 **Incident Closure and Evaluation**

11.6.1 All logged incidents that have been completely resolved must be formally closed and signed-off by the incident assignee and the user.

11.6.2 All logged incidents and their status must be reviewed by the Management on a regular basis.

11.6.3 All logged incidents must be subjected to periodic reporting to ensure that the incidents have been resolved in a timely manner and the correct solutions applied.

11.6.4 Senior Management should be provided with the following information on a periodic basis at least once a month:

a) a summary analysis of all logged incidents and causes distinguishing all incident by priority;

b) a summary report of the times taken to respond to the logged incident;

c) an ageing analysis of all outstanding logged incidents by priority;

d) a detailed analysis of all logged incidents exceeding their agreed resolution dates;

e) a detailed report of all incidents where the agreed resolution may affect service levels; and

f) any outstanding or unresolved incident.

12.0 BUSINESS CONTINUITY MANAGEMENT

OBJECTIVE

The objective of the requirements under Business Continuity Management is to minimize disruptions to the trading activities and operations of the POs from the effects of major failures of the critical systems or disaster.

12.1 Business Continuity Plan (BCP)

12.1.1 A BCP must be established to formalize the procedures and controls to ensure the required level of continuity of the business during adverse situation.

12.1.2 A BCP should be undertaken with business impact analysis to ensure that all key business activities, business support systems and operational functions are identified.

12.1.3 The responsibility for the development, documentation and implementation of the BCP must be defined, agreed and documented. The BCP must at least include the roles and responsibilities of the Plan Co-ordinator(s) and the respective team members.

12.1.4 Any services provided by third parties and their responsibilities must be formally defined and documented in a Supplier Agreement.

12.1.5 Personnel must be trained in the implementation of BCP procedures. Backup personnel must also be identified and trained.

12.1.6 Backup copies of the BCP must be kept securely off-site and there must be a policy established for access procedures.

12.1.7 All BCP must be kept up-to-date and reviewed at least on an annual basis. The review process must be documented and signed-off by management.

12.1.8 Any amendments to the BCP must be issued to all plan holders.

12.2 Testing of BCP

12.2.1 The BCP must be comprehensively tested to ensure that they are workable. Test plans must be developed and must at least include test objectives, scope, sequence of activities and timing/schedule. Problems arising during the testing and the actions taken to resolve these problems must be documented and reviewed.

12.2.2 Training should also be provided to all employee for any updates to the BCP and as refresher courses.

[End of Appendix 1]

DIRECTIVE ON THE PARTICIPATING ORGANISATIONS' DISASTER RECOVERY SITE STANDARDS AND THE IT SECURITY STANDARDS	**No. 5.05-001**

APPENDIX 2

PARTICIPATING ORGANISATIONS' DISASTER RECOVERY SITE STANDARDS (PODRS STANDARDS)

1.1 Disaster Recovery Site Standards and PO IT Security Standards

The objective of the establishment of a disaster recovery site is to facilitate the resumption of critical business operations within an acceptable timeframe in the event a disaster disables the computer and office facilities at the main business premise.

The following sections address the specific guidelines for the establishment of the disaster recovery site by Participating Organisations ("POs") to ensure that the above objective is met. However, POs are required to comply with the PO IT Security Standards for their full implementation, i.e. the PODRS Standards must be complied with in conjunction with the PO IT Security Standards.

POs are required to abide by these guidelines to achieve a minimum standard for the establishment of a disaster recovery site. However, POs may introduce more stringent and sophisticated measures to provide for higher levels of disaster recovery capability within their own organizations.

(1) <u>LOCATION OF DISASTER RECOVERY SITE</u>

(a) POs should ensure that the disaster recovery site is located at least 10km from the main business premise to ensure that when the main business premise cannot be accessed for any reason, the disaster recovery site is still accessible.

(b) POs must ensure that the main business premise and the disaster recovery site do NOT share the same power sub-station.

(c) POs must ensure that the main business premise and the disaster recovery site do NOT share the same telecommunication exchange.

(d) POs must ensure that the disaster recovery site is secured and accessible 24 hours if the need arises.

(2) <u>BACKUP OF COMPUTER OPERATIONS</u>

(a) POs must have in place a backup system to cater for clearing and settlement operations during a disaster.

(b) POs must ensure that the data is backed up as follows:

(i) Latest copy of system and application programs are secured at the disaster recovery site. Whenever there are changes or enhancement to the system or application programs, a backup copy is kept or the necessary update to the disaster recovery site is done accordingly; and

(ii) Inventory records of all backup data, application programs, vital business records, backup media and operations manuals are maintained at the disaster recovery site.

(d) POs must maintain at least 1 CDS terminal setup at the disaster recovery site so that the CDS function can be carried out during the disaster.

(e) POs must maintain sufficient trading terminals to cater for trading during the disaster.

(f) All the trading facilities must be maintained offline at all times other than during the disaster period.

(g) POs should maintain the network configuration setup to provide a fault-tolerant network with redundancy. This setup must be able to provide continuous connection availability from the Exchange to the PO.

(3) DISASTER RECOVERY PLAN

The disaster recovery plan must consist of business impact assessment, roles and responsibilities, framework for decision making, detailed recovery procedures and regular maintenance, testing and training. The minimum level of standards must include the following:-

(a) POs must clearly identify and document computing resources and office facilities needed to support critical business functions.

(b) POs must assign specific personnel for the disaster recovery roles and responsibilities.

(c) A disaster recovery plan and documentation must contain the following information:

- decision making for declaration of disaster;
- contact list of key recovery personnel (during and after office hours);
- information on permanent personnel working at the disaster recovery site;
- procedures for declaring disaster;
- procedures for activating disaster recovery site;
- procedures for resumption of computing facilities at the disaster recovery site;
- procedures for retrieval of vital records (data, programs, documentation); and
- procedures for resumption of normal computing facilities and business operation at main site procedures on plan maintenance, testing and training.

(d) POs must conduct training and testing to familiarize recovery teams with the disaster recovery plan at least once a year.

(e) The disaster recovery plan must be kept up-to-date and reviewed at least once a year.

(f) The disaster recovery plan must be integrated with the business continuity plan.

[End of Appendix 2]