BURSA MALAYSIA DERIVATIVES BERHAD

Date : 10 March 2008	Trading Participant Circular : 14/2008

TRADING PARTICIPANT INFORMATION TECHNOLOGY SECURITY CODE ("IT SECURITY CODE")

1. Trading Participants are hereby advised of the IT Security Code which is issued pursuant to Rule 103 of the Rules of Bursa Malaysia Derivatives Berhad which shall take effect on **17 March 2008**. The IT Security Code is as set out in **ANNEXURE A** attached herewith.

2. Please be advised that where a Trading Participant is unable to immediately comply with any of the requirements set out in the said IT Security Code on the effective date, the Trading Participant is given six (6) months from the effective date of the IT Security Code i.e. up to **16 September 2008** to comply with the requirements contained therein.

3. The IT Security Code is introduced for the purpose of establishing and putting in place IT controls and procedures for Trading Participants. However, Trading Participants with existing documented controls and procedures are not necessarily required to re-write a new set of controls and procedures. Where there are gaps or inconsistencies in the Trading Participants' existing documented controls and procedures based on the IT Security Code issued herein, the gaps or inconsistencies must be addressed in accordance with the IT Security Code.

4. This circular is available on Bursa Malaysia's website at http://www.bursamalaysia.com/website/bm/rules_and_regulations/bursa_rules/bm_derivatives.html.

5. For further information or any enquiries on the IT Security Code, kindly contact :-

   (a) Mr Pasupathy Velauthah (+603-20347141)
   (b) Mr Lum Chee Wah (+603-20347734).

RULE DEVELOPMENT & ADVISORY

ANNEXURE A

BURSA MALAYSIA DERIVATIVES BERHAD

TRADING PARTICIPANT INFORMATION TECHNOLOGY SECURITY CODE - BASELINE PROCEDURES

TABLE OF CONTENTS

[1] No Baseline Procedure has been developed for this Standard. It has been included here for completeness.

IT SECURITY BASELINE PROCEDURES

INTRODUCTION

Compliance to the IT Security Standards is compulsory to the extent that the computer equipment and Information Technology facilities are within the control of the Trading Participant.

Detailed IT Security Procedures must be implemented to achieve these Standards. It is the responsibility of each Trading Participant management to develop and document procedures in line with their operations.

APPLICATION OF BASELINE PROCEDURES

Baseline Procedures have been developed to assist in the development and identification of appropriate controls and procedures to meet the IT Security Standards in the Information Technology Security Code. These Baseline Procedures must be tailored to reflect the operational processes within each Trading Participant.

Trading Participants with existing documented procedures are not necessarily required to re-write a new set of procedures. Where there are gaps in their existing documented procedures, these Baseline Procedures can be used to assist in enhancing their procedures.

Baseline Procedures have been developed for the following Standards:

ITSS 2	: Personnel
ITSS 3	: Logical Access Controls
ITSS 4	: Physical Security and Environmental Controls
ITSS 5	: Installation Management
ITSS 6	: Computer Operations
ITSS 7	: Computer Disaster Recovery Planning (CDRP)
ITSS 8	: Change and Configuration Management
ITSS 9	: Problem Management
ITSS 10	: Application Development Standards
ITSS 11	: Telecommunications
ITSS 12	: Local Area Network (LAN) and Microcomputers

IT SECURITY BASELINE PROCEDURES

Baseline Procedures are defined as follows:

- Baseline Procedures that include the word "must" are minimum controls that need to be established to satisfy the IT Security Standards. However, alternative procedures may be used to achieve the objectives of the mandatory Baseline Procedures.

- Baseline Procedures that include the word "should" are to be treated as statements of best practice. The implementation of these Baseline Procedures is highly recommended.

BURSA MALAYSIA DERIVATIVES BERHAD

TRADING PARTICIPANT IT SECURITY CODE - BASELINE PROCEDURES

ITSS 1

SECURITY MANAGEMENT

OBJECTIVE

The objective of these Security Management Standards is to establish an Information Security management structure which is appropriately defined, with agreed responsibilities, authorities and inter-relationships. A clear framework of authorities and responsibilities is necessary to ensure the successful implementation of the security objectives of the Trading Participant.

SCOPE

The Security Management Standards will apply to information systems and information technology facilities to the extent that it is within the control of the Trading Participants.

REFERENCES

ITSS 3: Logical Access Controls Standards

1.1 Framework of Responsibilities

a. **Responsibilities for the management and administration of information technology security must be defined and agreed. The following information technology security functions must be identified :**

<u>Security Management</u>

Overall responsibility for ensuring that the information technology security requirements are implemented in the Trading Participant.

<u>Security Administration</u>

Responsible for the administration of logical and physical access controls for computerised information systems and monitoring access violation attempt reports.

<u>Internal Audit</u>

Responsible for reviewing the adequacy of IT security and controls and monitoring compliance with the Information Technology Security Policy, Information Technology Security Standards and Procedures.

b. **For each application system, the following should be identified :**

<u>Data Owners</u>

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

<u>System Owners</u>

Management responsible for business systems, whether or not those systems use information processing facilities. A business system must have only one owner who is responsible for approving changes to the applications. Owners of the system software must be similarly responsible for approving change in their area.

Explanatory Notes

In most cases, the Head of Department is responsible for the department's system. However, where a system spans several departments (i.e. Human Resource, Finance and Accounting), there then exist more than one owner. The owner may wish to discuss with affected parties the impact of any proposed changes to the *system and user requirements. However for reasons of accountability, there should only be one ultimate owner appointed.*

System Users

Any persons or functions using the information processing facilities in the course of their normal duties.

System Providers

Functional groups providing information systems to System Owners and Users.

Procedure Owners

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

c. All staff must comply with the Information Technology Security Policy and Information Technology Security Standards.

1.2 Security Management Responsibilities

a. Security Management must be appointed with responsibility for :

i. addressing and assigning responsibility for high level issues that affect security,

ii. enhancing the Information Technology Security Policy and Standards when necessary,

iii. approving formal application for waivers of non-compliance with these Standards on advice of Security Administration.

b. Security Management must be an identified individual from the ranks of the Senior Management.

1.3 Security Administration Responsibilities

a. Security Administration must be appointed with responsibility for :

i. promoting security awareness and education,

ii. administration of access controls software,

iii. providing advice and guidance on the development, maintenance and implementation of these Information Technology Security Standards and Procedures,

iv. reviewing access rights on a regular basis to ensure compliance with these Standards,

v. monitoring and investigating security violation attempts.

b. Security Administration should not be assigned responsibilities which would conflict with their normal duties.

1.4 Internal Audit Responsibilities

a. Responsibilities for the role of Internal Audit in the management and implementation of information technology security must be agreed and defined, and must include :

i. monitoring compliance with the Information Technology Security Policy, Information Technology Security Standards and Procedures, and evaluating internal controls within the information systems,

ii. providing advice and guidance on the development, maintenance and implementation of these Standards and procedures,

iii. review adequacy of the Business Continuity Plan (BCP) and Computer Disaster Recovery Plan (CDRP) in place to allow recovery from a system failure and in the event of a disaster, resulting in a loss of the information technology services,

iv. reviewing activities of Security Administration and advising on other security related issues.

Explanatory Notes

A document defining the responsibilities of Internal Audit should be established. In smaller companies, a full-time Internal Audit department may not necessarily undertake this function. Where there is no full time Internal Audit department, this function should be undertaken by a person independent from day to day operations, for example the Compliance Officer.

b. **Internal Audit must always be a separate function from Security Management and Security Administration.**

c. **Internal Audit must report directly to the Audit Committee. In the absence of an Audit Committee, the reports must be tabled to the Board of Directors meeting.**

1.5 Segregation of Duties

a. **The minimum level of segregation of duties will depend on the size of the system under consideration. Where applicable, the following duties should be segregated:**

- **application development**
- **technical support**
- **computer operations**
- **quality assurance**
- **internal audit**
- **security administration**
- **user departments.**

1.6 Classification of Information

a. **Information and related systems should be classified in accordance with an Information Asset Classification Policy.**

1.7 *Data Owners*

a. **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 standing data,**

iv. **ensure that risk assessment for the data they are responsible for has been performed and the data assigned a security classification.**

v. **review access profiles at a minimum, once a year.**

1.8 *System Owner Responsibilities*

a. **System Owners must :**

i. **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,**

ii. **verify that the systems meet with users' requirements,**

iii. **ensure that system users are provided with training,**

iv. **in conjunction with Security Administration and Internal Audit, ensure that the controls required within the process are defined and agreed,**

v. **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

vi. his / her normal duties,

vii. review access profiles at a minimum, once a year.

b. In the majority of cases, the System and Data Owner will be the same. There may be instances where the System Owner is separately defined from Data Owner. In these instances, the Data Owner must authorise users to use system functions specifically to create, update, delete and read the data.

1.9 System User Responsibilities

a. System users must :

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

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

1.10 System Provider Responsibilities

a. 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,

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

iv. ensure that, in case of failure, all systems are provided with defined and agreed recovery procedures,

v. provide information systems services that are required by the System Owners and System Users.

1.11 Procedure Owner Responsibilities

a. 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,

iii. control the distribution of the procedures and ensure that users have an up-to-date copy of the procedures,

iv. ensure that the procedures conform to the Information Technology Security Policy and Standards.

PERSONNEL

OBJECTIVE

Information technology security measures rely on the honesty and capability of individuals. As a result, the Management should involve consideration of a number of Personnel issues.

SCOPE

The Personnel Standards apply to all employees of the Trading Participants.

These Standards should be applied in conjunction with existing in-house personnel/human resource standards.

REFERENCES

ITSS 1: Security Management Standards

PERSONNEL

2.1 Security Training

a. **Information security education must be provided to all new staff and reinforced on an on-going basis to create and maintain security awareness among the staff.**

Baseline Procedures

1) All new staff must be given security awareness training upon joining.

2) Reinforcement security awareness education should be given to all staff at least once a year.

2.2 Employment of Staff

a. **All applicants for sensitive positions must be subject to adequate investigation and review before being employed.**

Baseline Procedures

1) Sensitive departments, sections and positions within the organisation must be identified.

2) Investigation of career history and appropriate qualifications for positions must be conducted.

3) Provision of at least one reference which must be followed up.

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

5) Access rights for newly appointed staff should be restricted during their probationary period.

6) Contract staff should not be employed in areas that are highly confidential or that would increase the risk of a security exposure to an unacceptable level.

2.3 Intellectual Property Rights

a. **The terms of employment must establish the intellectual property rights over any designs, procedures or inventions which the staff develops during the course of employment.**

Baseline Procedures

1) The terms of employment must establish the rights over intellectual property which the staff develops during the course of employment, which must be acknowledged by the staff.

2.4 Termination of Employment / Transfers

a. **There must be prompt notification of all staff movements by relevant departments to Security Administration and prompt action taken to revoke or amend access rights.**

Baseline Procedures

1) Personnel must inform Security Administration and other relevant departments of all staff resignations, terminations and transfers.

2) Where the employment of a staff is terminated, all access rights must be revoked immediately and, where appropriate, the staff escorted from the premises.

3) Employees in sensitive positions who resign should be assigned to alternate duties or offered early separation. Access rights must be revoked on the date of the staff's departure.

4) Any common passwords/codes known by the staff, must be changed on the date of the staff's departure.

5) Human Resource department must ensure all keys, identification and access cards held by leavers are returned.

Explanatory Notes

Human Resource may delegate this function to the respective Head of Department but ultimately it is Human Resource that is responsible.

6) Leavers should be allowed to take only personal items from the premises.

7) Transfer of job responsibilities must be reviewed by the Security Administration and Data Owner.

Explanatory Notes

A user access matrix should be developed by the Data Owner listing all pre-agreed access profiles for designated job functions. The Security Administrator is responsible for the day to day administration of these profiles.

2.5 Roles and Responsibilities

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

Baseline Procedures

1) Job descriptions must include compliance with IT Security Policy and Standards.

2) Roles and responsibilities must be acknowledged by the staff.

2.6 Disciplinary Procedures

a. All employees must be informed of the disciplinary action(s) that may be taken in the event of being found to have committed a security breach.

Baseline Procedures

1) All employees must sign a contract of employment that establishes their duties with respect to both physical and information technology security and which states that security breaches will result in disciplinary action or dismissal.

2) The employment contract must include the following arrangements for all employees :

- a confidentiality undertaking relating to disclosure of information,

- the requirement to note and report any observed or suspected security weaknesses,

- the disciplinary procedures that will be followed for employees found to have violated the Information Technology Security Policy, Information Technology Security Standards and procedures.

Explanatory Notes

A separate document, for example in the form of a Security Handbook, can be made available to employees. Employees are required to read this document and to sign a "read and understood" agreement.

2.7 Penalties for Non-Compliance

a. After due enquiry, non-compliance or violation of the Information Technology Security Policy and Information Technology Security Standards must result in action that may include but not be limited to:

- **civil and/or criminal prosecution,**
- **termination of employment without notice,**
- **downgrading,**
- **suspension from work without pay for a period of not exceeding one (1) week,**
- **any other lesser punishment.**

2.8 Appraisal

a. All staff must be appraised regularly including an assessment of compliance to the Information Technology Security Policy, Information Technology Security Standards and Procedures.

Baseline Procedures

1) The staff appraisal process must include an annual assessment of compliance with the Information Technology Security Policy, Information Technology Security Standards and Procedures.

2.9 Use of Contractors

a. **Work undertaken by contractors/third party service providers must be subject to compliance to the IT Security Policy and Standards.**

Baseline Procedures

1) Contractors must sign a standard contract which includes a requirement that any work undertaken on behalf of the Trading Participant must comply with the Information Technology Security Policy, Information Technology Security Standards.

2) Contractors must sign a statement of confidentiality.

3) Contractors must inform the Trading Participant of all other concurrent or known pending engagements that might present an actual or apparent conflict of interest.

4) Contractors' work must be monitored by an authorised staff.

5) Contractors must be monitored by an authorised staff when in the premises.

6) Contractors should not be given sole responsibility for a project team management.

7) No project should become dependent upon the continued involvement of a specific contractor.

LOGICAL ACCESS CONTROLS

OBJECTIVE

The objective of Logical Access Controls Standards is to enforce the segregation of duties by ensuring that individuals can only access data and perform processing functions to which they have been authorised.

SCOPE

The Logical Access Controls Standards apply the information systems and information technology facilities to the extent that it is within the control of the Trading Participants.

REFERENCES

ITSS 1: Security Management Standards

ITSS 2: Personnel Standards

ITSS 8: Change and Configuration Management Standards

LOGICAL ACCESS CONTROLS

3.1 User Access Administration

a. Access to all information systems must be restricted to authorised persons. The responsibilities for the administration of logical access controls must be defined, agreed and documented.

<u>Baseline Procedures</u>

1) Access to all computer information systems must be restricted only to authorised persons, enforced by system logical access controls.

2) A logical access control policy must be formulated by System and Data Owners, and where possible, administered by an independent Security Administration function. Based on the principle of least rights, the logical access control policy must define the access rights appropriate for each user group. This must be documented, e.g. in the form of an access control matrix. The access control policy should be based on the requirements of the business, taking into account:

   - the security requirements of the business application concerned,
   - the corporate and departmental policies for information dissemination and entitlement,
   - contractual or legal requirements to protect access to data or services.

3) Logical access controls must be used to enforce segregation of duties between incompatible functions. The following principles must be observed :

   - IT staff must not have access to end-user functions.
   - System and application programmers must not have routine access to production data, production systems or production application software.

4) Logical access procedures for the creation, amendment and maintenance of user and resource profiles must be defined, agreed and documented. Relevant audit trails for each of these activities must be maintained.

5) System enforced logical access paths should be implemented, such as the use of restricted menus and sub-menu options available depending on the individual user access profiles defined.

6) User access granted to system resources and application functions must only be granted on the basis of written requests authorised by System or Data Owners, which must be retained as an audit trail.

7) The System and Data Owners must ensure access rights are appropriately allocated. When authorising access, they must consider:

- compatibility with other responsibilities and existing access rights of the user,
- the classification of the information to be accessed,
- whether the requested level of access is required in order to allow the user to carry out his/her normal duties,
- duration of access required if granted on a temporary basis.

8) Security Administration must review all access requests. If Security Administration considers an access request as inappropriate, the matter must be raised with the System or Data Owner, who must provide additional written justification for the access request before its implementation by Security Administration.

9) Remote access to third party service providers/vendors may only be granted upon approval by IT management. All remote access must be under the control of Security Administration. Remote users' activities must be logged and monitored. Reason for access, duration and appropriate authorisation must be recorded in the log.

10) Naming standards for disk storage, directory structures, file names, and user IDs should be defined to aid the implementation of security.

3.2 Access Control Software

a. Access control software should be implemented to enforce resource security and segregation of duties.

Baseline Procedures

1) Logical access to system resources should be controlled by Access control software.

2) All user exits in system and access control software must be adequately documented, authorised and independently reviewed.

3) Access to access control software administration facilities must be limited to Security Administration.

3.3 User Identification

a. Computer information systems must require each user to identify him/herself to the system with a recognised approved user ID.

Baseline Procedures

1) Each authorised user of information systems must be designated a user ID to initiate terminal sessions.

2) A common user ID naming convention should be adopted across all computer platforms to facilitate the identification of individual users.

3) Users must not allow other persons to use their user IDs to gain access to computer resources.

4) User IDs should not be shared.

5) Default user IDs provided with the system software must either be disabled or have their passwords changed.

3.4 User Authentication and Password Protection

a. Computer information systems must require users to authenticate their identity by requiring a password to be used in conjunction with their user ID.

b. User passwords must be subject to strict controls to ensure confidentiality.

Baseline Procedures

1) Each user ID must require a password to authenticate the user's identity to the computer system in order to gain access to computer resources.

2) All new users must be educated on the protection of passwords.

3) Users must report unauthorised access attempts and unauthorised violation attempts to their respective Head of Department and Security Administrator.

4) Users must keep their passwords secret at all times. Users must be instructed not to divulge, print or write down passwords.

5) Access control systems should ensure that a minimum length for passwords, at least 4 characters in length.

6) Passwords must not be displayed on-screen during input.

7) Passwords must be kept encrypted within the system.

8) Users must be instructed to define passwords that are not easy to guess, i.e.:

- passwords must not be the same as the user ID,
- passwords must not be composed of repeating characters,
- passwords should not be the staff's, family or pet names or car registration numbers etc.,
- passwords should not be re-used,
- passwords should be composed of both alphabetical and numeric character combinations.

9) Passwords must be changed regularly for all systems and under the following conditions :

- at least every ninety (90) days for mission critical systems,
- upon first logon or when a new or amended password is issued by Security Administration. Where possible, systems should enforce password change upon first logon for new users,
- when a default password is provided with the system,
- where users suspects that their password is known to others,
- when there is staff termination or resignation,
- when user access rights change due to change in user responsibilities.

10) Logical access controls systems should enforce password changes by automatic expiry. Where this is not technically possible, passwords must be changed manually. In such situations, new passwords must be conveyed directly to users in a secure manner and users must acknowledge receipt of passwords.

11) Where possible, systems should prevent re-use of recent or similar passwords.

12) Users must be instructed that different passwords must be used where more than one layer of security exists.

13) The system log-on sequence should display the date and time of the user's last access to the system, and the number of failed access attempts since the last successful log-on.

3.5 Revocation of Access Rights

a. Access rights no longer required for an individual's normal duties must be revoked immediately.

Baseline Procedures

1) In the event of termination of employment, logical access rights assigned to the individual must be removed immediately.

2) In the event of resignation, logical access rights assigned to the individual must be reviewed , and where appropriate reduced or removed.

3) In the event of a change in user responsibilities, access rights must be reviewed and revised where appropriate.

4) User IDs must be deactivated/disabled if they are inactive for a period in excess of ninety (90) days.

   Explanatory Notes

   Where systems permit, deactivation of inactive user IDs (non-usage for more than 90 days) must be automated.
   Otherwise, there must be appropriate manual procedures to remove inactive user Ids.

5) User IDs for staff who are absent for an extended period of time, e.g. on maternity, sick or long term leave, should be deactivated.

6) User IDs should be automatically disabled after three (3) consecutive unsuccessful log-on attempts.

7) User IDs that have been automatically disabled must only be reactivated by Security Administration after an investigation has been conducted. The findings from the investigation must be documented.

3.6 Terminal Session Control

a. Logical access controls should be enforced to ensure that active terminal sessions are restricted to usage by authorised users.

Baseline Procedures

1) All users must be educated to log-off when leaving their terminals unattended for any period of time.

2) Unattended terminals should be automatically logged off or the screen ”blanked out” by a screen lock facility after a period of ten minutes inactivity. A password must be required before the terminal session can be reactivated.

3) Individuals must be required to re-enter their password after an active session has been deactivated as a result of a system failure, session time-out or other similar event.

4) The simultaneous log-on of two or more terminals using the same user ID should be prohibited. Where possible, the system should enforce this. During log-on, the system should inform the user if the user ID is already in use.

3.7 Monitoring of Access

a. Access to sensitive data, powerful utility programs and access violation attempts must be monitored, logged and investigated.

<u>Baseline Procedures</u>

1) Update access to files required on an emergency basis must be logged and the logs subject to retrospective review by Security Administration. Configuration Management should ensure that emergency changes conform to the Configuration Management Standards and Application Development Standards.

2) Access to sensitive data must be restricted. All access must be logged and subject to review by Security Administration.

3) Powerful utility programs capable of bypassing logical access controls must be:
   - stored in secure libraries,
   - restricted to a minimum number of authorised users,
   - protected from being copied or renamed.

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

5) All unauthorised access attempts and other security related events must be logged and should be subjected to review by Security Administration. Logging, reporting and surveillance facilities must be used to monitor security and should include:

   - logging of unauthorised access attempts,
   - logging of maintenance to security profiles or security tables,
   - logging of the use of sensitive commands,
   - logging of privileged user activity,
   - logging of access by third party vendors / engineers,
   - logging of access to system log file.

6) Users must not be able to modify audit logs.

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

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

3.8 Review of Access Profiles

a. **Logical access profiles must be reviewed on a regular basis, at least once a year, to ensure that access rights remain appropriate.**

Baseline Procedures

1) Logical access controls must be reviewed on a regular basis by Security Administration. As a minimum, the review must be undertaken at least once a year.

2) Business users' access profiles must be reviewed as a minimum once a year by the System or Data Owner.

3) A copy of the list of access profiles must be signed by the System or Data Owner and sent to Security Administration for filing.

PHYSICAL SECURITY/ENVIRONMENTAL CONTROL

OBJECTIVE

The objective of Physical Security/Environmental Controls Standards is to prevent unauthorised access to computer related equipment and to ensure that the computer related equipment is adequately protected against natural hazards and malicious damage.

SCOPE

The Physical Security/Environmental Controls Standards apply to the information systems and information technology facilities to the extent that it is within the control of the Trading Participants.

REFERENCES

ITSS 1: Security Management Standards

ITSS 3: Logical Access Controls Standards

ITSS 6: Computer Operations Standards

4.1 Physical Access to Data Centre

a. Physical access to computer and related equipment must be adequately controlled and restricted to authorised staff only.

Baseline Procedures

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

2) The siting of all critical computer related equipment must be in secure locations (Data Centre) to ensure that physical access is controlled.

3) These locations must not be publicly identifiable or visible from the outside and inside of the building.

4) Entrances to secure locations and sensitive areas must be fitted with locking devices, which should be able to identify staff and date and time of entry/exit.

5) Access to secure locations and sensitive areas must be restricted only to authorised staff.

6) Access to secure locations and sensitive areas by others (for example, third party contract staff, cleaning staff and maintenance engineers) must be controlled to ensure that :

   - they are bona fide,
   - they have been authorised by the contractor,
   - they have been approved by the relevant head(s) of department,
   - they are monitored by a member of staff.

7) Access by visitors and non-authorised staff to secure locations or sensitive areas must be authorised and logged. Such access must be supervised by an authorised staff.

8) The date and duration of visits must be recorded in a visitor's log which should be reviewed regularly. Security Administration is responsible for monitoring and administrating physical access into the Data Centre.

9) All emergency exits from the Data Centre must be equipped with alarms. Access to computer facilities in the Data Centre through these exits from the outside must be prevented.

10) Access to air conditioning units, power and telecommunication lines, and back-up power units must be secured.

11) Perimeter walls surrounding the Data Centre should be constructed from true floor to true floor.

4.2 Fire Safety and Water Supplies

a. **Computer and related equipment must be adequately protected from fire and water damage.**

<u>Baseline Procedures</u>

1) The Data Centre and areas containing critical computer related equipment and information systems staff must be protected by an automatic fire detection and alarm system.

2) Installation of fire suppression systems must comply with local regulations.

3) Fire detection and suppression systems must be inspected to ensure that they have been properly installed. The systems must also be inspected and serviced regularly, at least once a year.

4) Appropriate portable fire extinguishers must be placed in strategic locations. There must be no obstruction to these locations and the instructions for operating the fire extinguishers must be clearly displayed.

5) Smoking, eating and drinking must be prohibited in the Data Centre.

6) Electrical peripherals, for example distribution box and wiring, must be maintained by qualified electricians on an annual basis.

7) Main shut off valves for water sprinkler systems should be easily accessible.

8) All items and flammable materials not essential to Data Centre operations should be kept outside the Data Centre.

4.3 Power Supplies

a. **Power supplies to critical systems must be protected and backup sources provided to ensure continuity of processing.**

The Data Centre power supply must be backed-up as follows:

Generator required	**-**	**Data Centre air conditioning and lighting.**
UPS/Battery Backup required	**-**	**all computers, security and fire detection systems.**

Baseline Procedures

1) A generator must be installed as a back up power supply for the Data Centre.

2) Critical systems must be supported by an uninterruptible power supply (UPS) or have battery back up. Back up power supply must be able to support critical system load for at least a minimum period of ten minutes.

3) The generator and UPS must be securely located. Where possible, it should be located in a separate locked room and the key kept under secure conditions, accessible only to authorised personnel.

4) The location of the generator and UPS must be well ventilated and be equipped with fire detection and prevention systems.

5) Generator and UPS installations must be subject to regular inspection, maintenance and testing.

6) All electric cables must be laid and maintained in accordance with Jabatan Bekalan Elektrik (JBE) regulations.

4.4 Environmental Controls

a. The environment of the Data Centre must be properly controlled and monitored to ensure the efficient performance of computer and related equipment to reduce the risk of system failure.

Baseline Procedures

1) Room temperature in the Data Centre must be controlled within a specified range as recommended by the manufacturers of the computer equipment and peripherals.

   Humidity of the air in the Data Centre should also be maintained within a specified range as recommended by the manufacturers.

2) Adequate ventilation must be provided for all work areas. Air cooling units must be subjected to regular inspection and cleaning.

4.5 Control of Storage Media

a. **Access to computerised storage media must be restricted only to authorised staff and must be adequately protected from physical and environmental damage.**

Baseline Procedures

1) Access to computerised storage media, both on-site and off-site must be controlled and only granted to authorised personnel.

2) All movements of computerised storage media from storage must be logged. Proper authorisation(s) must be in place for movements to off-site locations.

3) Computerised storage media must be physically secured and protected from physical and environmental damage (e.g. fire, heat and water damage).

4) Computerised storage media must be rendered unreadable before disposal.

5) Storage media containing original installation software must be securely kept.

4.6 Printed Output

a. **Access to confidential printed output and printers generating confidential information must be restricted only to authorised staff.**

Baseline Procedures

1) Confidential information must be identified and documented.

2) Confidential information must be printed on secure printers (i.e. housed in secure locations).

3) Access to secure printers must be restricted and confidential printed output only released to authorised persons.

4) Documents containing confidential information must be rendered unreadable prior to disposal (e.g. cross-shredding).

4.7 Emergency Procedures

a. **Emergency and evacuation procedures must be documented. Staff must be adequately trained to handle emergencies.**

Baseline Procedures

1) Emergency and evacuation procedures should be documented and made available to all staff.

2) All staff must be informed of the emergency procedures. The emergency procedures must be tested at least once a year. Fire drill training must be given to designated individuals who will function as fire marshals in the event of an emergency.

3) Staff must be trained in the use of fire extinguishers.

4) First-aid supplies and emergency hand-held lights must be available and easily located.

5) Fire exits, evacuation rules, emergency power-off points, and location of fire extinguishers must be kept free from obstruction.

6) Procedures for safe evacuation in an emergency must be visibly posted at key locations.

BURSA MALAYSIA DERIVATIVES BERHAD
TRADING PARTICIPANT IT SECURITY CODE - BASELINE PROCEDURES

ITSS 5

INSTALLATION MANAGEMENT

OBJECTIVE

The objective of the Installation Management Standards is to ensure that system software and hardware are managed in a consistent and controlled manner in order that application systems are operated in a controlled manner.

SCOPE

The Installation Management Standards apply to all information systems and information technology facilities to the extent that it is within the control of the Trading Participants.

REFERENCES

ITSS 1: Security Management Standards

ITSS 4: Physical Security / Environmental Controls Standards

ITSS 6: Computer Operations Standards

ITSS 8: Change and Configuration Management Standards

INSTALLATION MANAGEMENT

5.1 System Software and Technical Support

a. Systems software must be installed and maintained for optimum performance according to vendors' recommendations, and must be adequately protected from unauthorised access.

Baseline Procedures

1) System software must be adequately protected by access control mechanisms.

2) All systems software must be fully supported by the vendor or an agent of the vendor. For example, operating system in use must be supported by the vendor.

3) All changes to system software must be authorised and processed in accordance to the Change and Configuration Management standards.

4) The vendor's proprietary update control software should be used to apply system software changes in accordance with the Change and Configuration Management Standards.

5) Any facility developed to automate system software maintenance must be fully documented and supported.

6) Any system failures and dumps must be logged, investigated and reported to IT management, in accordance with Problem Management Standards.

7) Details of instructions given by software support personnel to operations personnel must be documented in a log.

8) Requests for software support must be logged, detailing reasons for the request and personnel involved. When technical support personnel require temporary access to live data or software libraries for diagnostic purposes, the access request must be subject to authorisation and logged.

9) An inventory listing uniquely identifying all system software must be maintained and verified on a regular basis.

5.2 Hardware Management

a. Physical computer and related equipment must be properly controlled and maintained to ensure efficient performance and to prevent loss or damage.

Baseline Procedures

1) All computer and related hardware must be maintained in accordance with the Physical Security / Environmental Controls Standards.

2) An inventory list uniquely identifying all computer and related equipment must be maintained and verified on a regular basis.

3) The removal, movement or disposal of computer equipment must be authorised and logged, in accordance with Change and Configuration Management Standards.

4) Hardware maintenance agreements must be established for computer equipment. All such agreements must include preventive maintenance.

5) All computer equipment must be operated and maintained in accordance to the manufacturer's specifications.

6) A log of hardware problems and actions taken to resolve the problems must be maintained, logged and reviewed, subject to Problem Management Standards

7) Hardware capacity planning must be performed and reviewed on a regular basis, at least once a year.

5.3 Service Level Agreements with Third Party Service Providers

a. Service Level Agreements (SLAs) must be established between Trading Participants and third party computer service providers to formally define the agreed service performance standards and course of action in the event of service support failure.

Baseline Procedures

1) For all outsourced services, formal Service Level Agreements (SLAs) must be established and agreed between third party computer vendors and Trading Participants.

2) SLAs must document, where applicable, the following :

- Start and end dates for the SLA
- Responsibilities of the parties, including accountability for assets managed by service provider
- Confidentiality undertaking
- Days and hours of service availability
- Means of contacting key personnel
- Maximum response times
- Activity monitoring, information to be reported and method of reporting by vendor

- Mechanisms to ensure compliance, including penalties for non-performance and termination procedures
- Definition of terms
- Billing arrangements
- Equipment required
- Operations and user contact personnel
- Relevant standards
- Compliance with IT security requirements
- Escrow agreement, where necessary
- Ownership of all resources, where necessary
- System availability (within and outside of normal business hours), where applicable
- System performance (including on-line response times, on-line and off-line printing and batch completion times), where applicable
- Capacity requirements, where applicable
- Recovery times, where applicable
- Contingency arrangements (availability and performance), where applicable.

3) All IT staff and affected parties must be made aware of the relevant SLAs and the commitments contained within.

4) The response time for vendor support must be defined and agreed upon, and must correspond to the required levels of availability of systems as defined in the SLAs.

5) System performance must be regularly monitored against levels defined in the SLAs.

6) SLAs must be reviewed on a regular basis, at least once a year.

7) SLAs must be subject to Change and Configuration Management Standards. SLAs must be amended to reflect system and installation changes or business needs.

5.4 Procurement of Hardware and Software

a. Hardware and Software procurement procedures must be developed to ensure that the best equipment and software available to meet business requirements is used. All IT hardware and software must be compatible.

Baseline Procedures

1) A list of approved equipment and vendors should be maintained.

2) Hardware and software procurement procedures must be developed to control all procurement of IT hardware and software (including PC products).

3) The selection of computer equipment must be authorised by IT management.

4) All procurement of hardware and software including “free of charge” supplies must be performed in consultation with the IT department.

BURSA MALAYSIA DERIVATIVES BERHAD TRADING PARTICIPANT IT SECURITY CODE - BASELINE PROCEDURES	ITSS 6

COMPUTER OPERATIONS

OBJECTIVE

The objective of Computer Operations Standards is to ensure that operational procedures are documented and adhered to. These operational procedures are to ensure the continuity of processing, minimising the risk of disruption to computer services and to ensure that jobs are processed in an authorised manner.

SCOPE

The Computer Operations Standards apply to all information systems and information technology facilities to the extent that it is within the control of the Trading Participants.

REFERENCES

ITSS 1: Security Management Standards

ITSS 4: Physical Security / Environmental Controls Standards

ITSS 7: Computer Disaster Recovery Planning Standards

ITSS 8: Change and Configuration Standards

ITSS 9: Problem Management Standards

COMPUTER OPERATIONS

6.1 Operating Instructions

a. **Operating instructions must be properly documented and available to operations staff to ensure the smooth operation of computer equipment and to ensure that processing is performed as authorised.**

Baseline Procedures

1) All Computer Operations instructions must be approved and documented. These should include :

- staff responsibilities
- maintenance and upkeep of environmental, computer and related equipment
- responses to program and system messages
- authorised job control schedules
- job run procedures
- backup procedures and media management
- recovery and restart procedures
- emergency procedures.

2) All documentation in Computer Operations must be maintained and regularly updated by Computer Operations staff to ensure information is up-to-date, complete and accurate. This should be subject to review by management.

6.2 System Logs

a. **System activities must be logged and monitored for irregularities.**

Baseline Procedures

1) A log of system activities, including the operator console activity, where applicable, must be maintained as an audit trail and reviewed.

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

3) The system log:

- must be archived until all outstanding problems which require reference to it have been resolved, afterwhich it may be purged;
- should be archived for a minimum period of at least one year; and
- should be audited.

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

6.3 Data Centre Environment

a. A safe and secure Data Centre environment must be maintained to ensure the physical security of data and computer equipment.

<u>Baseline Procedures</u>

1) The Data Centre environment must be maintained in compliance with the Physical Security / Environmental Controls Standard.

2) All Computer Operations staff must be trained to deal with emergencies (such as fire or bomb threats) and in the discharge of manual and automatic fire extinguishing systems.

3) Smoking, eating and drinking must be prohibited in the Data Centre.

6.4 Backup Storage Media Protection

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

<u>Baseline Procedures</u>

1) Copies of back-up files and documentation must be kept in a secure off-site location at all times. Backup copies must be transferred to the off-site location regularly, preferably daily.

2) Security of backup storage media must be maintained in compliance with the Physical Security / Environmental Controls Standards.

3) Off-site locations must be subject to the defined Physical Security / Environmental Controls Standards

4) Off-site locations must be situated at a reasonable distance from the primary computer site.

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

6) Centralised inventory listings of all storage media must be maintained for both on-site and off-site locations. Details recorded must include:

- unique label name of the media item and contents;
- the location; and
- the data retention period of the storage media.

7) Inventory checks must be carried out, at least once a year to ensure that all storage media are accounted for. There should be periodic testing of backup media at both on-site and off-site locations to ensure that back-ups are in useable condition for recovery and that their contents are as documented. Back-up media found to be unreadable must be reported to the Head of Computer Operations.

8) All movements of back-up media must be monitored and logged. The deposit and withdrawal of back-up media from storage locations must be restricted to only authorised staff.

9) Copies of back-up files moved to or from off-site storage locations must be provided with defined and agreed levels of security during transportation.

10) The retention period of back-ups must be defined and agreed by Computer Operations, Systems and Data Owners in accordance with relevant regulatory requirements. These must be documented in operations procedures.

11) All media containing confidential data must be rendered unreadable prior to removal or disposal.

12) The removal or disposal of all storage media must be authorised and logged.

13) When computer equipment is changed, consideration should be given to the back-up media and data formats to ensure that they can still be restored.

14) Back-up media must be capable of being retrieved within a specified timescale as documented in the Computer Disaster Recovery Plan.

15) Where a third party has been authorised to store back-up media, a service level agreement (SLA) should be defined and documented, and in compliance with the IT Security Standards.

6.5 Frequency and Retention of Backups

a. Backups should be made on a regular basis that will ensure the continuity of processing in the event of a processing interruption.

Baseline Procedures

1) The frequency of data back-ups and their retention period must be defined and agreed by Computer Operations, System Owners, Data Owners and Application Development. These must be documented in the operations procedures.

2) Back-ups must be made prior to and after any major changes to the system or application software.

6.6 Job Scheduling and Reporting

a. Job runs must be monitored against approved job schedules, and all problems and exceptions must be reported and reviewed.

Baseline Procedures

1) Production jobs must be run in accordance with an authorised job schedule. Job schedules must be completed, independently reviewed and retained as an audit trail. The console log must be independently reconciled to the authorised job schedule on a regular basis.

2) All ad-hoc jobs must be authorised by business and IT management.

3) Shift reports must be kept to ensure a smooth hand-over from one shift to another. Any emergency jobs or reruns must be logged, and the reasons for any changes to the authorised schedule recorded in the shift report.

4) The shift reports must be reviewed by the Head of Computer Operations or a nominated staff.

5) All problems must be logged with the details of actions taken, in accordance with Problem Management Standards.

6.7 Segregation of Duties

a. Computer Operations function must be segregated from the development function.

Baseline Procedures

1) Computer operations must not have access to utilities, development tools and source programs that would permit them to by-pass logical access controls, or to alter production data or programs in an unauthorised manner.

6.8 *Security over Computer Reports*

a. Access to computer reports generated, or in the print queue, must be restricted to authorised staff to ensure the confidentiality and integrity of data.

Baseline Procedures

1) Security over computer reports must be maintained in compliance with the Physical Security / Environmental Controls Standards and Logical Access Control Standards.

2) Access to spooled files must be controlled to prevent alteration or disclosure of confidential information.

6.9 *Recovery and Restart*

a. Procedures must be defined and documented to ensure the recovery of data and systems within the shortest acceptable time, following a system or transaction failure. Staff must be trained in these procedures.

Baseline Procedures

1) Management must define the minimum recovery time for each critical business application.

2) The Computer Operations manual must define recovery and restart procedures. Operations staff must be trained in these procedures

3) Recovery and restart procedures must be tested prior to implementation in production systems. These must be tested at least once every six months.

4) On-line transaction systems that update data in the primary computers should permit recovery up to the last successful transaction in the event of a system or transaction failure.

5) The integrity of data must be verified after recovery procedures have been completed before restarting system services.

6) Authorisation to restore data from back-up media that would overwrite existing production data must be obtained from the Data Owner(s).

ITSS 7

COMPUTER DISASTER RECOVERY PLANNING

OBJECTIVE

The objective of the Computer Disaster Recovery Planning Standards is to ensure the resumption of business support systems within an acceptable time frame in the event of a disaster.

SCOPE

The Computer Disaster Recovery Planning Standards apply to all information systems and information technology facilities to the extent that it is within the control of the Trading Participants..

REFERENCES

ITSS 1: Security Management Standards

ITSS 4: Physical Security / Environmental Controls Standards

ITSS 6: Computer Operations Standards

ITSS 8: Change and Configuration Management Standards

COMPUTER DISASTER RECOVERY PLANNING

Explanatory Notes

- *Business Continuity Planning consists of 2 aspects: computer related disasters and the impact on business operations. As such, contingency plans must include a Business Contingency Plan (BCP) and Computer Disaster Recovery Plan(s).*

- *Computer Disaster Recovery Planning must be undertaken to ensure the prompt recovery of business support systems in the event of a computer related disaster.*

- *Business Continuity Planning must be undertaken to ensure the continuity of business operations in the event of a disaster.*

- *For the purposes of the Information Technology Security Standards, the focus is on Computer Disaster Recovery Planning although elements of the standards can also be suitable for BCP.*

7.1 Responsibilities for Computer Disaster Recovery Planning (CDRP)

a. Senior management must ensure that Computer Disaster Recovery Planning is undertaken for the continuity of business.

<u>Baseline Procedures</u>

1) A Computer Disaster Recovery Plan (CDRP) must be developed and maintained for critical computer facilities.

2) Responsibility for the development, documentation and implementation of the CDRP must be defined, agreed and documented. The CDRP must at least include the role and responsibilities of the Plan Co-ordinator(s) and the respective team members.

3) Any services provided by third parties and their responsibilities must be formally defined and documented in a Service Level Agreement (SLA). Please refer to Change and Configuration Management Standards - Service Level Agreements.

4) Staff must be properly trained in the implementation of CDRP procedures. Backup staff must also be identified and trained.

5) The CDRP must be kept classified as confidential organisational data.

6) The CDRP 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 by the Recovery Co-ordinator.

7) Back-up copies of the CDRP(s) must be held securely off-site, and there must be access procedures in place.

7.2 Scope and Contents

a. The scope and contents of the CDRP must be adequate to ensure the continuity of key business activities.

Baseline Procedures

1) Computer Disaster Recovery Planning should be undertaken with business impact analysis to ensure that all key business activities, business support systems and operational functions are identified.

2) The CDRP must be documented. It should at least include the following :

- notification and invocation procedures,
- directory of CDRP team members, civil authorities, relevant third parties and service level agreements and the emergency contact numbers for all parties,
- index classification of the range of disaster events,
- inventory listings and configuration documentation,
- inventory of backup media and access procedures,
- provision for back-up facility which is secure and accessible 24 hours,
- detailed procedures for resumption of operations at the back-up facility,
- detailed procedures for resumption of operations at the primary site from the back-up facility,
- priorities for tasks and restoration of processing,
- interim/emergency manual operating procedures for business operations.

7.3 Maintenance

a. All CDRP must be kept up to date and reviewed and tested at least once a year.

Baseline Procedures

1) All CDRP 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.

2) A list of the mission critical configurations must be maintained on an ongoing basis in support of the Business Continuity Plan. This must be in accordance to Change and Configuration Management Standards.

3) CDRP must be regularly tested. Testing should be performed on a partial basis, but all components of the plan must be tested at least once every two years. Test plans must be developed and documented. Test results must be documented and reviewed.

4) Staff training should also be provided to new staff for any updates to the CDRP, and as refresher courses.

5) Any amendments to the CDRP must be issued to all plan holders.

7.4 Insurance

a. **Insurance cover should be obtained to protect against losses arising as a consequence of failure of the computer systems and the business in the event of a disaster.**

Baseline Procedures

1) Adequate insurance cover must be obtained to cover all valuable assets, these must include all assets required to support business operations.

2) The insurance policy should cover all equipment at all locations including telecommunications equipment and personal computers.

3) The insurance policy should consider the additional cost of the use of back-up equipment such as cost of accommodation, additional travel expenses, overtime, etc. all of which are likely to be incurred should a disaster occur.

4) The insurance policy should cover consequential loss in the event of a disaster.

5) There must be procedures to ensure that the insurance policy is kept up-to-date with the latest acquisitions, and reviewed at least once a year.

6) The insurance policy must be for replacement value of assets and not for historical or second-value.

CHANGE AND CONFIGURATION MANAGEMENT

OBJECTIVE

The objective of the Change and Configuration Management Standards is:

to establish a framework to maintain a continuous record of the status of hardware and software items. This is to ensure that changes to Trading Participants' systems are implemented in a controlled environment and in a consistent manner; and

to ensure a means of identifying and controlling the individual components/configuration items that together constitute the Trading Participants' systems (i.e. to know what components comprise any given system, whether those components are undergoing changes and where those components are at any given point in time).

Definition of Configuration Item:

Configuration item refers to any individual hardware or software item that comprises the Trading Participants' information systems and support infrastructure.

Definition of Change:

- a new configuration item acquired, or
- a movement of an existing configuration item, or
- removal of a configuration item,

whether between physical and/or logical environments.

SCOPE

The Change and Configuration Management Standards apply to all information systems and information technology facilities to the extent that is within the control of the Trading Participants.

REFERENCES

ITSS 1: Security Management Standards

ITSS 5: Installation Management Standards

ITSS 6: Computer Operations Standards

ITSS 7: Computer Disaster Recovery Planning Standards

ITSS 10: Application Development Standards

8.1 *Configuration Item Identification*

a. **All configuration items must be tracked and properly controlled in their respective lifecycles.**

Baseline Procedures

1) Approved inventory listings uniquely identifying all configuration items must be maintained. Inventory listings must include details of item name, identification code, short description, ownership (e.g. department), location of the item, and relationship to other configuration items where applicable.

2) Configuration documentation must provide the following information:

   - System/project to which the item relates and the location.
   - Creation date, current version and the versions of components of the item and status.
   - Description and status of changes made to the configuration item.
   - Name of the item, identification code and the nature of the function or service that the item provides, where appropriate.
   - Tools and environment used to create the configuration item. This will ensure that compatibility is increased and regression errors are avoided.

3) Configuration diagrams and documentation on configuration items and the relationship between dependent configuration items must be maintained and updated on a regular basis.

4) All procurement of configuration items (including PC products) must be made in accordance to the hardware and software procurement procedures.

8.2 *Configuration Lifecycles and Logical System Environments*

a. **Lifecycles for hardware and software configuration items must be established to enable their status to be tracked at any point in time.**

b. **Logical system environments must be defined to support each of the main lifecycle stages of all software configuration items.**

Baseline Procedures

1) All configuration items must be recorded to facilitate the identification of its location and status at any point in time.

2) Lifecycles for hardware configuration items must be established, to at least include:

   - acquisition,
   - commissioning,
   - production (deployment).

3) Lifecycles for software configuration items must be established to at least include:

   - Development
   - Test
   - Production

4) Logical system environments must support each of the main lifecycle stages of all configuration items. Separate environments should be established for, at least, the following:
   - Development
   - Test
   - Production

5) Each hardware platform must have their logical system environments documented by Configuration Management.

6) The logical system environments must be periodically checked as part of quality assurance.

7) The logical system environments must support the segregation of incompatible duties between IT functions and end-user functions.

   Where applicable, the following duties within the IT activities must be segregated:
   - Computer Operation;
   - Technical Support;
   - Application Development.

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

9) For externally developed software, an additional receiving environment must be established. This will enable quality control to be carried out prior to its movement to either the acceptance or production environments.

10) The Systems Test and Acceptance Test environments should be consistent with the Production environment, to ensure adequate levels of confidence in the testing.

11) Production program source codes should be kept in a secure library with restricted access. Programmers must not have write access to production source.

12) The transfer of modified software configuration items to the production environment must be carried out by a function independent of the development function.

13) Access to each environment must be restricted to authorised persons only. The access granted must be the minimum access that is necessary for that person to carry out their authorised activities.

8.3 Change Management

a. All changes to the systems must be properly assessed, authorised, tested and implemented. The change lifecycle must be properly documented to provide an audit trail.

Baseline Procedures

Change Initiation and Authorisation

1) All changes must be in compliance with the Installation Management Standards.

2) All proposed changes to configuration items must be formally authorised by the owner of the item, IT management, and the relevant System and Data Owners.

3) Prior to authorising any significant proposed changes, management must assess the impact of a proposed change, including the impact on system stability or security. All areas potentially affected must be identified, including all activities, users, systems, standards, contingency plans and insurance policies, and all affected parties must be consulted prior to implementation of the change.

4) Changes should be classified and documented as (1) application system changes, or (2) technical changes - hardware or software. Emergency changes for these categories should be documented as such.

5) All changes must be performed on the basis of formal written instructions. The written instructions must set out:

- The confirmation to be changed (item identification code, version, author)
- description of the change
- name of requestor and date of request
- who has authorised the change

- reason for the change, reference to other relevant documentation where appropriate
- assessment of impact and when the change is required to be completed by
- how the change is to be carried out (e.g. appropriate build and compilation requirements)
- authorisations
- name of assignee handling the change request
- the criteria that must be applied to determine whether the change has been completely and accurately made
- date of implementation.

Change Implementation

6) All changes must be subjected to adequate formal testing and acceptance. All changes must be supported by the appropriate sign-off to confirm that the relevant quality control criteria have been met prior to implementation.

7) All changes of configuration items must be documented and an audit trail must be created. The audit trail must record the history and current status of a change item and must be established to link the change history for the item to the relevant change/movement request instructions.

8) Advance notice must be given to those affected by the change to enable them to take appropriate action in response to a change. If insufficient time is provided, then the reason must be formally documented.

9) All affected hardware and software configuration documentation, manuals, contingency plans and insurance policies must be updated.

10) The transfer of modified configuration items to the production environment must be carried out by a function independent of the development function and only on receipt of written authorisation.

11) Written instructions, including fallback procedures must be provided for each transfer into production.

12) Backup and version controls must be in place.

Software change management

13) Controls must be in place to ensure that the compilation and build process are valid and authorised when system programs or applications are moved into the production environment.

14) For application software items, object codes should not be transferred between logical system environments.

15) Where software is implemented at remote locations then:

- the location of all versions must be formally documented
- the configurations on which they have been installed must be formally documented
- for software that communicates directly with the Trading Participant's system, its integrity must be confirmed at each host authorisation and authentication session.
- the integrity of each update of the software must be confirmed at the time of update and controls established to confirm the integrity and completeness of the update.

8.4 Change Management for Third Parties

a. Changes implemented or received from third parties must be subject to the Change and Configuration Management Standards.

Baseline Procedures

1) Third party must formally schedule and communicate all deliveries of configuration items.

2) Sufficient notice must be given to enable appropriate levels of impact analysis and quality control to be conducted, and to communicate the impending receipt of the configuration items to all affected parties.

3) Prior to accepting of the change, a reconciliation must be performed of the delivered items to the vendor's statement and authorised requirements to confirm the completeness and accuracy of what has been delivered.

4) Adequate documentation to must be provided to install, operate and maintain the configuration item without needless recourse to the vendor. In the event that the software has been customised, documentation must be appropriately amended.

5) Proper instructions must be available to back out the installation of the configuration items in the event of a failure.

6) Delivered configuration items should be accompanied by statements from the vendor that the quality of the items have been confirmed by a Quality Assurance function.

7) Sign-offs must be obtained at each of the relevant stages of the item's change management lifecycle. Relevance should depend on the nature of the configuration item (e.g. packaged software, turnkey, in-house developed software or some combination of the three). For turnkey systems, the sign-offs should comply with the Application Development Standards. For packaged software, the Application Development Standards should be used

to evaluate the vendor's application system and should be the minimum basis by which the implementation and maintenance is carried out.

8) Acceptance of the configuration items from third parties must be formally signed-off by the item owner, System and Data Owner after all the Configuration Management quality controls have been satisfied.

8.5 Emergency Change Control

a. **Emergency changes implemented must be subject to retrospective authorisation and review to ensure that such fixes do not compromise the security and integrity of the Trading Participants' systems.**

Baseline Procedures

1) Change and Configuration Management Standards must be retrospectively applied to all emergency changes.

2) Emergency changes must be carried out in the presence and under the review of a person independent of the one making the change.

3) An emergency change report must be prepared by the person making the change and verified by the independent reviewer, at the time of the emergency change.

4) Emergency access must be obtained using dedicated emergency user profiles.

5) Access to dedicated emergency profiles must be available at all times and should be under dual control.

6) Emergency maintenance to production software must be carried out in accordance with Application Development Standards with the exception that these Standards may be applied retrospectively.

7) The emergency change report, where applicable, must detail:

- the reason for the change
- what was changed and when it was changed
- why the change was classified as an emergency change
- the testing, verification or quality controls that were applied prior to the change
- method of implementation, including back-out procedures and locations
- who was informed of the change and the name of the independent reviewer
- how access to the system was obtained, indicating the profiles, system authorities and utilities used
- whether the change was successful or not.

8) Emergency change reports, where applicable, must be accompanied by the following documentation:

- the operations incident log
- an audit log of the commands issued and activities carried out by the person making the emergency change, where possible
- any test results or other system generated information to confirm the integrity of what was done
- a statement from the independent reviewer to confirm that:
  - the information provided in the report is complete
  - the person making the change did not change the information in the report
  - the report is consistent with their understanding of the incident
  - they were present for the full duration of the emergency access
  - the profiles used to make the change were disabled immediately after completion of the change.

9) All emergency changes must be monitored by Security Administration and subjected to retrospective review and approval.

10) All emergency changes must be communicated to all parties that are affected by the change.

8.6 Back-up and Business Continuity Planning

a. Configuration management process must be established to facilitate effective recovery of the systems in the event of a disaster.

Baseline Procedures

1) A backup of all configuration items:

- must be taken on a periodic basis, sufficient to enable:
  - the restoration of a previous configuration to any point in time within either statutory requirements or company requirements whichever is the greater
  - restoration of the current configuration within agreed recovery timescales.
- should be taken on a periodic basis, sufficient to enable the restoration of a previous version of a configuration item to any point in time within three versions

2) The frequency with which back-ups are taken and the back-up strategy employed, must be determined in conjunction with Computer Operations, Application Development and System and Data Owners.

3) Back-ups must be made prior to and after any changes to the production environment.

4) Back-ups must be capable of enabling the change to be reversed within agreed timescales to maintain the required level of operational service and recovery times.

5) Back-ups should be expiry date protected.

6) A list of the mission critical configurations must be maintained on an ongoing basis in support of the Business Continuity Plan.

7) The back-up strategy for each system must be formally documented and approved by the System and Data Owners.

8) All back-ups must be stored in a secure location that is documented and consistent with the Computer Disaster Recovery / Business Continuity Plan's requirements.

9) Back-up media must be periodically tested and replaced at appropriate intervals. The back-up intervals must be determined in conjunction with manufacturer's guidelines, having due regard to the nature of the information stored.

8.7 Reporting and Quality Management

a. Trading Participants' systems must be baselined at defined events and regular intervals to ensure the ongoing effectiveness of Configuration Management.

Baseline Procedures

1) A configuration baseline audit should be periodically performed to ensure that Change and Configuration Management Standards and Procedures are followed, and to ensure the integrity of configuration management documentation.

2) Each baseline should be backed-up and stored according to the Computer Disaster Recovery / Business Continuity Plan.

3) The configuration baseline must be reconciled to the actual configuration and the Computer Disaster Recovery / Business Continuity Plan copy.

4) Configuration baselines must be updated for any changes i.e. :

- when there are new software releases,
- immediately following scheduled Computer Disaster Recovery / Business Continuity Plan tests,
- when there are operating system upgrades,

- at each quarter-end.

5) The Configuration Management reports must detail:

- number of changes performed,
- number of successful and unsuccessful changes,
- status of all incomplete changes,
- number of emergency changes,
- number of on - time and late deliveries from external vendors,
- time lost due to normal changes,
- time lost due to emergency changes,
- rejected changes,
- configuration item changes that did not conform to the Standards,
- an aged summary of all outstanding deliveries, summarising why the delivery is late and the action taken to resolve the issues.

PROBLEM MANAGEMENT

OBJECTIVE

The objectives of Problem Management Standards is to establish a system for recording, diagnosing and resolving all problems identified during production in a consistent, controlled and timely manner.

SCOPE

The Problem Management Standards will apply to information systems and information technology facilities to the extent that is within the control of the Trading Participants.

These do not address the systems or procedures for recording and controlling problems in the application development lifecycle.

REFERENCES

ITSS 1: Security Management Standards

ITSS 8: Change and Configuration Management Standards

ITSS 10: Application Development Standards

PROBLEM MANAGEMENT

9.1 Problem Recording and Prioritisation

a. All production problems must be formally recorded in a consistent format in a central location.

Baseline Procedures

1) Each recorded problem must be uniquely identified and centrally recorded in a Problem Log to be monitored by the Problem Management function.

2) Each record must contain only one problem to enable each individual problem to be tracked.

3) Access to the Problem Log must be restricted to authorised staff.

4) For each recorded problem, the following information must be detailed including:

   - a summary description of the nature of the problem,
   - the date and time the problem was identified,
   - the extent of the problem and its implications on other components of the system,
   - how it was identified / who reported (name/dept),
   - the configuration item names affected by the problem (e.g. program identifiers, report identifiers, terminal identifiers, etc...),
   - the priority of the problem.

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

9.2 Problem Assignment and Diagnosis

a. All recorded problems must be promptly assigned to the appropriate staff for diagnosis and correction.

Baseline Procedures

1) All Problem Management staff must review the Problem Log at the start of each working day and ensure that all problems assigned/escalated are attended to.

2) Each recorded problem must be assigned to an individual support staff, i.e. the “problem assignee”. The name of the problem assignee must be documented in the Problem Log.

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

4) The problem assignee must ensure that each recorded problem has been correctly classified in respect of priority.

5) The problem assignee must notify the Problem Management function of the expected date of problem resolution. The date of resolution must be agreed with the relevant System/Data Owners concerned.

6) Action to resolve a problem will depend on the priority (high, medium or low) and must be initiated within defined time limits.

7) If the problem assignee cannot diagnose the cause or find a suitable solution, the problem must be escalated to the Problem Management function. Unresolved problems must be escalated by the Problem Management function within the defined time limits.

9.3 Problem Resolution

a. All problems must be resolved on a timely basis according to their priority and agreed dates of resolution.

Baseline Procedures

1) All problems must be resolved according to their priority and agreed dates of resolution.

2) The problem assignee must promptly inform the Problem Management function of any delay to the agreed resolution dates and provide revised estimates.

3) The action taken to resolve the problem must be documented in sufficient detail to enable an independent person to analyse the actions taken without recourse to the problem assignee.

9.4 Problem Reporting and Review

PROBLEM MANAGEMENT

a. **All reported problems must be subject to periodic management review to ensure that problems are resolved in a timely manner and the correct solutions applied.**

<u>Baseline Procedures</u>

1) All problems reported and their status must be reviewed by IT management on a regular basis.

2) All problems must be recorded in a form that is in sufficient detail to enable their status to be ascertained at any point in time.

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

- a summary analysis of all problems recorded and causes distinguishing all problems by priority
- a summary report of the times taken to respond to the problem
- an aged analysis of all outstanding problems by priority
- a detailed analysis of all problems exceeding their agreed resolution dates
- a detailed report of all problems where the agreed resolution may affect service levels
- any unresolved problems.

	BURSA MALAYSIA DERIVATIVES BERHAD **TRADING PARTICIPANT IT SECURITY CODE - BASELINE PROCEDURES**	**ITSS 10**

APPLICATION DEVELOPMENT

OBJECTIVE

The objective of Application Development Standards is to establish a framework for ensuring that application software is developed, implemented and maintained in a structured and consistent manner.

SCOPE

The Application Development Standards will apply to all software that is created, implemented or maintained by the Trading Participants.

Where software is developed by third parties then these Standards should be the minimum criteria by which development, implementation and maintenance is carried out.

If the software is acquired by the Trading Participants, these Standards should be used for evaluating the vendor's application system and should be the minimum criteria by which the implementation and maintenance of the acquired software is carried out.

The Application Development Standards are the baseline by which the Systems Development Lifecycle is applied. The methods, tools or techniques by which this lifecycle is carried out are not addressed in this document.

REFERENCES

ITSS 1: Security Management Standards

ITSS 8: Change and Configuration Management Standards

BURSA MALAYSIA DERIVATIVES BERHAD
TRADING PARTICIPANT IT SECURITY CODE - BASELINE PROCEDURES

ITSS 10

APPLICATION DEVELOPMENT

OVERVIEW

Achievement of these Standards ensures that:

- an appropriate management and quality control structure is applied to all software development, implementation or maintenance activities,
- end-user requirements are documented and understood,
- requirements analysis is carried out,
- design is carried out according to defined requirements,
- code, data and systems are constructed in a structured and maintainable format,
- adequate levels of testing are carried out to confirm that the user requirements have been met and that no regression errors have been introduced,
- all of the implementation aspects set out below have been addressed:
    - scheduling instructions
    - user training
    - data conversion
    - performance and capacity verification,
- quality assurance activities are carried out.

10.1 Project Management

a. **For all projects, the Project Manager, System Owner and Data Owner(s) must be identified and the project must be led by adequate management involvement. The Project Manager should be identified from the management team.**

b. **A Systems Development Lifecycle Methodology must be adopted. The Methodology must extend from the selection/feasibility stage to the implementation stage. All projects must be conducted based on the Methodology and all projects must be managed and operated based on this Methodology.**

c. **A Project Plan must be developed for all projects to ensure that they are properly planned with proper assignment of responsibilities (including quality control) and resources, project timetables which are revised periodically, identification of project milestones, in compliance to the defined methodology.**

10.2 Systems Development LifeCycle and Project Planning Methodology

a. **The Systems Development Lifecycle Methodology must specify as a minimum, the definition of the lifecycle stages, the sign-off checkpoints during the lifecycle, documentation standards, security requirements, testing levels, conversion and implementation controls.**

Baseline Procedures

1) The Systems Development Lifecycle methodology must define as a minimum:

- the stages within the lifecycle by which progress can be monitored.
- the documentation and deliverables to be produced at each stage. This should include:
  - feasibility study/analysis to address project scope, business justifications, key business and technical requirements and documenting an analysis of various solutions and a cost-effective solution recommended;

- testing documentation to ensure conduct comprehensive testing and ease of maintenance;
- conversion and implementation documentation.

2) Formal sign-off must occur at the end of the key stages defined in the system lifecycle process.

3) This sign-off must identify, where applicable, the:

- System/Data Owner,
- System Provider (IT Management),
- Security Administration,
- Internal Audit,
- Quality Assurance.

10.3 Project Planning

a. A project plan must be prepared for all major projects (to consider cost, time, third party involvement and criticality of systems when determining "major").

Baseline Procedures

The project plan must identify:

- the key stages and tasks within the lifecycle of the software development,
- the people assigned to the project, their roles and responsibilities,
- the dates on which each project activity will commence and complete,
- the tangible deliverables and documentation to be produced,
- the extent of quality control,
- training for users and other staff,
- post-implementation review requirements.

10.4 Feasibility Study

a. An approved feasibility study, signed off by System Owner and IT management must be performed for major projects (to consider cost, time, third party involvement and criticality of systems when determining "major").

Baseline Procedures

1) The feasibility study should include a description of :

- scope/boundaries,
- business justification,
- business problems/issues,
- current processing procedures,
- estimation of operating cost and weaknesses,
- options available to address the problems/issues (this may include a technical description, advantages and disadvantages, cost/benefit analysis and an assessment of how the proposed option will address known weaknesses),
- resource requirements (adequacy of maintenance and support),
- recommended solution.

10.5 Requirements Analysis and Design

a. Requirements analysis must be performed to ensure that user functional and technical requirements are defined and documented in sufficient detail for application development.

Baseline Procedures

1) User requirements must be specified, documented and signed-off by the System Owner. This should include a description of :

- the business processes and details of processing functions,
- the computerised controls which should be implemented in the new system.

2) Technical systems requirements must be specified, documented and signed-off by IT management. The technical specifications must describe in detail how the system will be built, how it will operate, the organisation of data, access method and system processing.

3) Requirements analysis must include how existing business processes and systems will be affected by the new application.

4) Requirements analysis must address the following quality characteristics :

- functionality (business, user, regulatory, interface, security requirements),
- usability (human interface requirements),
- reliability (operational reliability and recovery requirements),
- maintainability (documentation for maintenance requirements),
- portability (conformance with operating systems, network and hardware requirements),
- efficiency (resource and performance requirements).

5) All requirements must be specified in sufficient detail to enable functional and technical aspects to be addressed in application development.

6) Logical, physical and data design specifications to implement the approved user and technical requirements must be developed, documented and approved.

10.6 Construction

a. Adequate controls must be in place to ensure that software is properly constructed and documented.

Baseline Procedures

1) Development of programs must be performed on the basis of formally agreed specifications and programming standards.

2) Source codes must be documented to enable its purpose, processing and change history to be ascertained without reference to additional documentation. Source code must also be referenced to the program specifications documentation.

3) Program coding specifications, where applicable, must be maintained for each program constructed or updated. These must include:

- program number, version control number and version date,
- version of the application development language,
- general description,
- author's name,
- files used by the program,
- program dataflow identifying inputs, processes and outputs,
- any special compilation requirements and program dependencies.

4) There should be independent review of program code.

10.7 Testing

***a.* Adequate testing must be completed to ensure that user requirements have been correctly and completely implemented into the new/amended application system.**

Baseline Procedures

1) All new or amended application software must be subjected to formal testing. This must consist of :

   - unit testing
     (to confirm the functional correctness of the developed software)

   - systems testing
     (to confirm the software works as specified when integrated with other programs and systems that it interfaces with, and to confirm that developed software has not introduced errors to programs/systems that were previously reliable)

   - acceptance testing
     (to confirm that the defined requirements have been met)

   - operational testing
     (to confirm that the application can be operated to agreed service levels and with adequate level of security)

2) Testing strategies must be based on defined specifications and business and system requirements established and documented in a test plan.

3) Responsibilities for test activities must be specified in the test plan.

4) The testing environment must be subject to Change and Configuration Management standards.

5) Test scripts, test data, expected and actual test results must be fully documented.

6) All problems/issues identified must be recorded into the problem log during the user acceptance test phase and integration test phase.

7) The testing process should include an acceptance test of the entire system which must include computerised functions, security and control features, and must also confirm the accuracy of associated user and operational procedures and documentation.

8) Final test results should be independently reviewed at a management level.

9) Acceptance criteria must be defined, documented and formally approved by System Owner and IT management. Acceptance criteria must be precisely stated, objective and measurable and must include the following:

   - testing and test documentation,
   - system performance/capacity,
   - operational scheduling and job control,
   - training and documentation,
   - user acceptance,
   - data conversion,
   - software migration.

10.8 Conversion Procedures

a. **Controls over data conversion must be in place to ensure the accuracy and completeness of the data in the new system.**

Baseline Procedures

1) An approved data conversion plan must be defined, documented and signed off by the System/Data Owner for movement of data into a new/amended system.

2) User controls must be in place to check the accuracy and completeness of the data in the new/amended system. The System/Data Owner must sign-off the results of the conversion process.

10.9 Implementation

a. **Adequate controls must be in place to ensure that all activities necessary to complete the application development lifecycle have been carried out.**

Baseline Procedures

1) There must be formal System Owner and IT management authorisation to ensure that all testing and documentation is completed, reviewed and problems rectified satisfactorily.

2) Prior to implementation, formal sign-off must be obtained by the Security Administrator and Project Manager.

3) Internal Audit should ensure:

- that the System Development Life Cycle process have been satisfactorily carried out;
- signed-off by the various responsible parties; and
- the relevant IT Security Standards have been complied with for major projects.

4) All user and operations training must be fully conducted prior to implementation.

5) Implementation of new/amended applications into the production environment must be subject to Change and Configuration Management Standards.

10.10 Documentation

a. **Adequate documentation must be maintained for the entire systems lifecycle.**

Baseline Procedures

1) Documentation must cover the entire systems lifecycle, including the security measures implemented.

2) Adequate documentation must be produced and retained to enable an independent audit of the system lifecycle process.

10.11 Backup, Version Controls and Security of Logical System Environments

a. **Proper backup and version controls must be in place for all program code, documentation, data structures and test data in all stages of the lifecycle. As a minimum requirement, version numbers should be given to indicate the status.**

b. **Change and Configuration Management Controls Standards must be complied with to control the movement of software between test and production environments.**

c. **The security of logical system environments must be enforced and maintained throughout the system lifecycle, from program construction, testing and implementation.**

10.12 Quality Assurance

a. **Quality assurance must be undertaken to ensure that the Application Development Standards have been complied with and in an effective manner.**

Baseline Procedures

1) There must be quality assurance in all stages of the systems lifecycle. This should be a function independent of application development, where possible.
2) All projects should be subject to a post-implementation review.

10.13 Application Controls

a. Requirements analysis must include an analysis of security requirements within the application system. These should focus on the automated controls to be incorporated within the system and the supporting manual controls.

Baseline Procedures

1) Security requirements for application systems must be defined, documented and approved by System/Data Owners, Internal Audit and Security Administration.

2) Security requirements should reflect the business value of the information assets involved and the potential business damage which might result from a failure/absence of controls.

3) Security requirements for application systems must consider the need for the following controls:

   - access controls to protect confidentiality, integrity and availability of data, and to enforce the segregation of duties,

   - input data edit/validation controls. The following should considered:

     - validation of input data against masterfiles
     - invalid/missing/incomplete data or characters
     - field combination checks
     - out-of-range characters or volume limits
     - check digits
     - controls totals for batch input,

   - audit trails of transactions and key events,

   - integrity controls during processing. The following should be considered:

     - session/batch controls to reconcile data file balances after updates
     - balancing controls to check opening balances against previous closing balances, e.g. run-to-run controls, file update controls, program-to-program controls
     - validation of system generated data

  - integrity checks on data transfers between computers,

- backup and recovery capabilities, including fallback processing arrangements,
- data encryption for highly sensitive data,
- compliance to legislation and other regulatory requirements.

TELECOMMUNICATIONS

OBJECTIVE

The objective of Telecommunications Standards is to ensure that transmitted data is protected against loss, corruption or repetition and unauthorised disclosure and modification; and unauthorised access to the Trading Participants' systems is not gained via the telecommunications network.

SCOPE

The Telecommunications Standards will apply to the telecommunications systems to the extent that is within the control of the Trading Participants.

REFERENCES

ITSS 1: Security Management Standards

ITSS 3: Logical Access Controls Standards

ITSS 4: Physical Security / Environmental Controls Standards

ITSS 5: Installation Management Standards

ITSS 6: Computer Operations Standards

ITSS 8: Change and Configuration Management Standards

TELECOMMUNICATIONS

11.1 General Standards

a. Telecommunications network systems must be subject to Installation Management Standards.

b. Telecommunications network equipment must be located in secure locations in compliance with the Physical Security/Environmental Controls Standards.

c. Telecommunications network systems must be secured with logical access controls implemented in compliance with the Logical Access Controls Standards.

d. Telecommunications systems must be secured to ensure defined and agreed levels of data integrity, confidentiality and availability. Measures must be in place to ensure:

i. The integrity of messages for example, inclusion of automatic error checking and/or correction (parity checking, checksum, cyclical redundancy check) and retransmission functions in the network protocol.

ii. The confidentiality and authenticity of messages containing sensitive data during transmission, (for example by implementing data encryption and digital signatures). In order to determine the appropriate level of security, management must conduct a risk assessment of the data transmitted each time the nature of data changes significantly, such as when a new system is implemented. Information classified as confidential or restricted should be encrypted whilst transmission through the network.

iii. The integrity and confidentiality of configuration data, including keys for encryption, routing tables, terminal identifiers etc.

iv. The integrity and confidentiality of network data relating to users, for example, user ids and profiles, user locations, remote access numbers etc.

v. The availability of the network to the service level required by the users.

vi. The integrity of network management software and user profiles. For example, logical access controls to ensure access is restricted only to authorised network management personnel, proper installation and set-up.

vii. Network services and facilities are not used by unauthorised users (for example, by restricting access using user IDs and passwords, by using smartcards, call-back devices, firewalls etc.)

viii. Physical security over network equipment and lines, and selective use of secure transmission media.

ix. The auditability of the network via the provision of adequate audit trails, (for example notification to sender and to system audit trail of non-delivery in the event of failure, message logging etc.)

x. Security controls must be consistent across networks.

<u>Baseline Procedures</u>

1) Responsibility for network management and security administration must be defined and documented.

2) Encryption should be considered to ensure the confidentiality of messages containing sensitive data during transmission. Where encryption is used, all data encryption keys should be assigned an owner and subject to adequate protection. Encryption keys must not be written down or printed.

3) Network diagrams must be maintained, and should include details of circuits used and circuit reference numbers. All network components must be uniquely identifiable and restricted to their intended business functions.

4) A list of all network users and systems communicating via the network, must be maintained.

5) Where feasible, locations that require more than five external connections must use centralised concentrators or multiplexing equipment attached to a dedicated communications server for more effective network security administration.

6) The Trading Partipants’ internet connections should only be used for authorised business purposes.

7) Host processors running applications or containing non-public data must be protected from public external networks using firewalling techniques.

8) Network management documentation must be made available to operators, kept up to date and restricted to authorised network management and operations staff.

9) All failures of network equipment must be reported to the Problem Management function.

10) All changes to the network configuration must be authorised and subject to Change and Configuration Management Standards.

11) Network capacity planning and performance analysis must be conducted at least once every six months.

11.2 Network Management

a. **Management of Telecommunications network systems must be conducted in a controlled and consistent manner in accordance with Change and Configuration Management Standards and Problem Management Standards.**

Baseline Procedures

1) Responsibility for network management and security administration must be defined and documented.

2) Encryption should be considered to ensure the confidentiality and authentication of messages containing sensitive data during transmission. Where encryption is used, all data encryption keys should be assigned owners and subject to adequate protection. Encryption keys must not be written down or printed.

3) Network diagrams must be maintained, and should include details of circuits used and circuit reference numbers. All network components must be uniquely identifiable and restricted to their intended business functions.

4) A list of all network users and systems communicating via the network, must be maintained.

5) Where feasible, locations that require more than five external connections must use centralised concentrators or multiplexing equipment attached to a dedicated communications server for more effective network security administration.

6) The Trading Partipants' internet connections should only be used for authorised business purposes.

7) Host processors running applications or containing non-public data must be protected from public external networks using firewalling techniques.

8) Network management documentation must be made available to operators, kept up to date and restricted to authorised network management and operations staff.

9) All failures of network equipment must be reported to the Problem Management function.

10) All changes to the network configuration must be authorised and subject to Change and Configuration Management Standards.

11) Network capacity planning and performance analysis must be conducted at least once every six months.

11.3 Network Resilience

a. **Contingency plans must be established for all critical telecommunications network systems to ensure the stability of the network and to ensure a fast and efficient recovery in the event of a system failure.**

<u>Baseline Procedures</u>

1) Methods of recovery from a network failure must be defined and documented in the Computer Disaster Recovery Plan and designed as part of the overall Business Continuity Plan and should include:

- Availability of spare telecommunications equipment on demand
- Procedures for activating back-up equipment units
- Availability of alternative communication lines to provide dynamic re-routing of messages
- Availability of uninterruptible power supplies or alternate power sources
- Use of multiple communication carriers
- Formal agreement on contingency service levels with tele-communications hardware and software vendors
- Documentation of recovery procedures

11.4 Network Physical Security

a. **Physical security over telecommunications components must be in compliance with Physical Security / Environmental Controls Standards and Change and Configuration Management Standards.**

<u>Baseline Procedures</u>

1) Physical Security/Environmental Control Standards must be applied to all components of the network.

2) The routes followed by cables from the point of entry to the premises of the Trading Participants should be secured.

3) Telecommunications equipment should be housed in a room separate from the other computer equipment and access to these rooms must be restricted to authorised persons.

4) Activities of external parties involved in installing, repairing, or servicing telecommunications equipment must be monitored by authorised staff.

5) A register of the telecommunications equipment and software must be kept and periodic reconciliations made to reconcile the reported assets with their physical availability and location.

11.5 Network Logical Access Controls and Monitoring

a. Access to all telecommunication network systems must be restricted to authorised persons, in compliance to the Logical Access Controls Standards.

Baseline Procedures

1) The Logical Access Controls Standards must be applied to telecommunication networks. Users should be given access to specific network resources based on functional requirements and the need for segregation of duties.

2) All default passwords for network equipment and software must be changed upon installation.

3) Positive authentication of remote users must be established before a remote connection is allowed, i.e. the user must be positively identified through a login sequence requiring a user ID and password prior to allowing access.

4) Welcome messages for external network connections must not be displayed until the user is positively authenticated.

5) Dial-in facilities should be disallowed; dial-out facilities should be used instead. Where dial-in facilities are necessary, adequate controls must be implemented, such as use of call back verification.

6) Software that perform unattended file transfers to or from other systems must authenticate the origin and destination file names as well as any user submitting the request.

7) Routers must regulate traffic flow according to access control lists defined by the network security administrator, where possible.

8) Modifications to the network management software should be subject to Change and Configuration Management Standards.

9) Network management software should include the following features:

- security management with access protection (user authentication, resource security, firewall enabling) and monitoring of user activity and security violations
- monitoring capabilities to track and report network status, errors and statistics at the port and device level
- performance management features
- accounting for resource usage.

10) Diagnostic tools and other system software utilities must be restricted to authorised persons. For example, access to the network screen capture facility must be restricted to authorised staff who perform problem diagnosis and resolution.

11) Security reports should be produced and reviewed on a regular basis. It should include details of:

- Network user and resource profiles
- Network security violation attempts
- Audit trails
- Use of dial-up line

BURSA MALAYSIA DERIVATIVES BERHAD
TRADING PARTICIPANT IT SECURITY CODE - BASELINE PROCEDURES

ITSS 12

LOCAL AREA NETWORK AND MICROCOMPUTERS

OBJECTIVE

The objective of Local Area Networks (LAN) and Microcomputers Standards is to ensure that LAN and the use of Microcomputers are adequately managed, controlled and monitored.

SCOPE

The Local Area Network & Microcomputers Standards will apply to the Local Area Network & Microcomputer Systems to the extent that is within the control of the Trading Participants.

REFERENCES

ITSS 1: Security Management Standards

ITSS 3: Logical Access Controls Standards

ITSS 4: Physical Security / Environmental Controls Standards

ITSS 5: Installation Management Standards

ITSS 6: Computer Operations Standards

ITSS 7: Computer Disaster Recovery Planning Standards

ITSS 11: Telecommunications Standards

BURSA MALAYSIA DERIVATIVES BERHAD
TRADING PARTICIPANT IT SECURITY CODE - BASELINE PROCEDURES

ITSS 12

LOCAL AREA NETWORK AND MICROCOMPUTERS

12.1 Logical Access Controls

a. Access to all Local Area Network systems must be restricted to authorised persons and be established in compliance with Logical Access Controls Standards.

Baseline Procedures

1) All LAN access and security of system resources must be established in compliance with Logical Access Controls Standards.

2) Access to Supervisor/System Management functions and the assignment of security equivalences must be limited to network personnel and LAN System Administrators.

3) Access to LAN management software and sensitive network files must be restricted to the LAN System Administrator.

4) The access rights over network files must be reviewed at regular intervals to ensure they remain appropriate.

5) Gateway resources must be protected from unauthorised access and modification.

6) Positive identification of remote users must be established before a connection is allowed. Remote access to the LAN must be controlled in accordance with Logical Access Controls :

   - Dial- in access should not be allowed
   - Access controls must restrict the functions available
   - Where appropriate, dial back modems should be used.

7) Audit trails must be reviewed and appropriate follow-up actions taken. These must be documented.

8) The availability of functions which can be used to override system logging parameters must be restricted.

9) Workstations used to store sensitive information should be secured. Access control facilities provided with the application software packages must be used. Diskless workstations should be used where network data is considered sensitive to prevent copying and unloading.

10) Screen savers with passwords should be used to prevent unauthorised access to an unattended microcomputer.

11) Power up passwords should be enabled where available.

12) Data downloaded from host computers for use on microcomputers must have the similar level of protection as the original data.

13) An audit trail logging activities of workstations used for processing critical information should be maintained including details of programs executed. The audit trail should be reviewed regularly.

14) The installation default passwords for privileged and other standard system accounts must be changed. Guest, field service or temporary IDs to the LAN must be disabled or deleted when not in use.

15) Encryption must be used to protect LAN access passwords and sensitive files on the server.

16) Naming standards for disk storage, directory structures, file names and user IDs should be defined to aid the implementation of security.

17) Logging, reporting and surveillance facilities must be used to monitor security and should include:

- logging of unauthorised access attempts,
- logging of maintenance to security profiles or security tables,
- logging of the use of sensitive commands,
- logging of privileged user activity,
- logging of access by third party vendors / engineers,
- logging of access to system log file.

12.2 Physical Access Controls

a. Physical security over LAN and microcomputer systems components must be in accordance with Physical Security/Environmental Controls Standards and Change and Configuration Management Standards.

Baseline Procedures

1) The designated owner of the LAN and microcomputer hardware and software must be identified and be responsible for the security of the equipment and software. Relocation of the equipment from its original position must be based on written authorisation from the owner.

2) An inventory of all LAN and microcomputer systems components must be maintained in compliance with Change and Configuration Management Standards and should include details of ownership (e.g. department), software used and location of the components.

3) Controls over physical access to critical LAN components must be in compliance with Physical Security/Environmental Controls Standards and must include :

- locating the servers in secure rooms/cabinets with adequate environmental controls. These rooms must be restricted to authorised persons.

- allowing only authorised persons to operate the equipment.
- storing secondary media (for example diskettes and cartridges) securely.

4) Where possible, all unused ports must be disabled to prevent illegal access to the LAN.

5) External parties installing, repairing or servicing LAN and microcomputer systems equipment must be monitored by authorised IT staff.

12.3 LAN Management

a. Management of Local Area Network systems must be conducted in a controlled and consistent manner in accordance with the Installation Management Standards, Computer Operations Standards, Problem Management Standards and Change and Configuration Management Standards.

Baseline Procedures

1) LAN & Microcomputer Systems management documentation should be made available to staff responsible for the daily operation of the LAN.

2) The design, installation and maintenance of the LAN should include :

- compliance with recognised LAN protocols and standards,
- inclusion of automatic error checking functions in the network protocol,
- security issues of LAN interconnectivity (internal and external),
- appropriate use of specialised network components, such as bridges, routers and gateways,
- installation and testing of LAN hardware components,
- installation and testing of LAN software components,
- virus checking of all software loaded into the LAN,
- the provision of adequate maintenance arrangements.

3) Day-to-day operation of the LAN must be in accordance with Computer Operations Standards and should be defined to include :

- maintenance and administration of LAN security,
- control and monitoring of LAN hardware including unique physical identification of LAN components and maintenance of inventory registers,
- monitoring and reporting of LAN utilisation, performance and capacity planning,
- LAN problem reporting and resolution,
- back-up and recovery procedures,
- off-site data storage procedures.

4) A list of systems communicating via the LAN must be maintained.

5) All problems on the LAN & Microcomputer Systems must be reported to the Problem Management function and must be subject to Problem Management Standards .

6) Changes to the LAN & Microcomputer Systems must be authorised and subjected to Installation Management and Change and Configuration Management Standards.

7) The critical applications developed for LAN & Microcomputer Systems must be subjected to Application Development and Change and Configuration Management Standards.

8) All software installed on the LAN & Microcomputer Systems must be authorised and licensed.

9) Third party software must be installed according to vendor's instructions.

10) Unauthorised copying of LAN and microcomputer proprietary software must be prohibited.

11) Unauthorised changes to the LAN and Microcomputer Systems software must be prohibited.

12.4 LAN Resilience

a. Contingency plans must be established for all critical LAN systems, to ensure the stability of the LAN and to ensure a fast and efficient recovery in the event of a system failure.

Baseline Procedures

1) Computer disaster recovery plans must be established for all critical LAN systems, in accordance with Business Contingency Planning Standards.

2) Methods of recovery from a LAN failure should be formalised and should include :

- availability of spares devices with sufficient capacity and speed for back-up purposes; for example :
  - maintaining spare equipment on-site for critical LAN components e.g. LAN interface cards, cabling, connectors, terminators and bridge devices
  - adequate provision for the re-routing network messages in the event of a component failure,
- unique physical identification of LAN components to facilitate problem diagnosis,
- frequency and retention of backups of the servers and workstations,
- documentation and testing of back-up and recovery procedures,

- uninterruptible power supplies systems to protect critical network servers and LAN components,
- availability and use of back-up and recovery software.

3) Disk mirroring and duplexing should be used for servers processing critical business applications.

4) LAN backup media must be secured in accordance with Computer Operations Standards.

12.5 Control of Computer Viruses

a. Critical servers and workstations must be installed with antivirus software. Antivirus procedures must be developed to minimise the risk of computer viruses infecting and causing damage to data and programs.

Baseline Procedures

1) Antivirus software must be installed on all LAN servers and workstations/microcomputers to ensure that all directories and files are scanned regularly.

2) Antivirus software must be auto-executed upon login to the LAN and upon PC bootup.

3) All antivirus software must have the following features:

- virus detection and removal capabilities,
- licensing agreement which provides regular updates for new viruses at least every 6 months,
- reputable track record, in terms of reliability and the number and nature of viruses it can detect and remove,
- memory resident protection.

4) Antivirus procedures i.e. actions to taken in the event of virus infection must be defined, documented and all users informed of the procedures. The procedures should include the following:

- The suspect/virus infected diskettes must be isolated
- Suspect/Infected microcomputers must not be used until they have been cleaned
- The relevant IT support department must be informed
- All virus occurrences must be logged and treated as security incidents.

5) Virus checks must be made on all new and external diskettes.

6) Back-up copies of all software and data must be maintained to reload an infected system.

7) Software/data should not be passed to third parties without having checked that they are virus-free.

12.6 Microcomputers

a. Adequate controls must be placed over microcomputers used for processing sensitive data to ensure the confidentiality, integrity and availability of these systems. The controls should be in compliance with the Logical Access Controls Standards, Installation Management Standards, Physical Security / Environmental Controls Standards, Computer Operations Standards and Change and Configuration Management Standards, where applicable.

Baseline Procedures

1) Microcomputer systems must be subject to the Installation Management Standards, where applicable.

2) Microcomputers used for processing sensitive data must be secured or located in a secure location in compliance with the Physical Security / Environmental Controls Standards, where applicable. For example, hardware locks should be used to restrict access where necessary.

3) Microcomputers used for processing and storing sensitive data must be secured. Where applicable, it must be in compliance with the Physical Security/Environment Control and Logical Access Controls Standards.

4) Data downloaded for use on microcomputers must be provided with similar level protection as that provided for the original source data.

5) Master copies of software must be used for installation of the software. The master disks must be installed according to the vendor's instructions and stored securely in a separate location.

6) Data and program files must be regularly backed-up and backup media kept in compliance with Physical Security/Environmental Controls Standards and Computer Operations Standards where applicable.

7) Automated back-up functions within software packages should be used where available.

8) Movement of microcomputers must be subject to proper authorisation in accordance with Change and Configuration Management Standards.
9) Users must switch off their computer equipment before leaving the office premises.

Explanatory Notes

A consistent level of security for data must be maintained at all times.

For example:

- *If data cannot be changed in the original system and can be downloaded, then the downloaded data must be protected from changes.*

- *If confidential data is downloaded to a microcomputer, then access to the machine must be secured. The machine must also not have 'print' or 'copy to removable media' capabilities (i.e. diskless workstations).*