ICTA
INFORMATION & COMMUNICATION TECHNOLOGIES AUTHORITY

CONTROLLER OF CERTIFICATION AUTHORITIES (CCA)

Level 12, The Celicourt 6, Sir Celicourt Antelme Street Port Louis Mauritius
Tel.: (230) 211 5333/4 Fax: (230) 211 9444 email: info@cca.mu

CCA
CONTROLLER OF CERTIFICATION AUTHORITIES OF MAURITIUS

THE CCA DIRECTIVE 2 OF 2010

Ref: ICTA/CCA/CCAD/2/2010 **10 December 2010**

The Information and Communication Technologies Authority in the exercise of its function as the Controller of Certification Authorities and in pursuance of Section 18 (1) (z) of the Information and Communication Technologies Act 2001 (as amended), Section 37 of the Electronic Transactions Act 2000 (as amended) and Regulation 3 (3) of the Electronic Transactions (Certification Authorities) Regulations 2010, hereby issues the following Directive.

1. Short title and Commencement

(i) This Directive shall be called "The CCA Directive 2 of 2010 - (CCAD 2 of 2010)"

(ii) The CCA Directive 2 of 2010 shall come into effect on 13 December 2010.

2. Scope and objective

This Directive provides for the implementation and management of Information Technology Security practices to be adopted by licensed, recognised and approved Certification Authorities.

Information & Communication Technologies Authority
Level 12
The Celicourt
6, Sir Celicourt Antelme St
Port Louis

Mr. T. Dwarka
Chairman

Dr. M. K. Oolun
Executive Director

To: All Licensed, Recognised and Approved Certification Authorities

DIRECTIVE - II

Information Technology (IT) Security Directives

Index

Information Technology (IT) Security Directives

1. Introduction

This document provides directives for the implementation and management of Information Technology Security. Due to the inherent dynamism of the security requirements, this document does not provide an exact template for the organisations to follow. However, appropriate suitable samples of security process are provided for directives. It is the responsibility of the organisations to develop internal processes that meet the directives set forth in this document.

The following words used in the Information Technology Security Directives shall be interpreted as follows:

- shall: The directive defined is a mandatory requirement, and therefore must be complied with.

- should: The directive defined is a recommended requirement. Non-compliance shall be documented and approved by the management. Where appropriate, compensating controls shall be implemented.

- must: The directive defined is a mandatory requirement, and therefore must be complied with.

- may: The directive defined is an optional requirement. The implementation of this directive is determined by the organisation's requirement.

2. Implementation of an Information Security Programme

Successful implementation of a meaningful Information Security Programme rests with the support of the top management. Until and unless the senior managers of the organisation understand and concur with the objectives of the information security programme its ultimate success is in question.

The Information Security Programme should be broken down into specific stages as follows:-

(a) Adoption of a security policy;

(b) Security risk analysis;

(c) Development and implementation of a information classification system;

(d) Development and implementation of the security standards manual;

(e) Implementation of the management security self-assessment process;

(f) On-going security programme maintenance and enforcement; and

(g) Training.

The principal task of the security implementation is to define the responsibilities of persons within the organisation. The implementation should be based on the general principle that the person who is generating the information is also responsible for its security. However, in order to enable him to carry out his responsibilities in this regard, proper tools, and environment need to be established.

When different pieces of information at one level are integrated to form higher value information, the responsibility for its security needs also should go up in the hierarchy to the integrator and should require higher level of authority for its access. It should be absolutely clear with respect to each information as to who is its owner, its custodian, and its users. It is the duty of the owner to assign the right classification to the information so that the required level of security can be enforced. The custodian of information is responsible for the proper implementation of security directives and making the information available to the users on a need to know basis.

3. Information Classification

Information assets must be classified according to their sensitivity and their importance to the organisation. Since it is unrealistic to expect managers and employees to maintain absolute control over all information within the boundaries of the organisation, it is necessary to advise them on which types of information are considered more sensitive, and how the organisation would like the sensitive information handled and protected. Classification, declassification, labelling, storage, access, destruction and reproduction

of classified data and the administrative overhead this process will create must be considered. Failure to maintain a balance between the value of the information classified and the administrative burden the classification system places on the organisation will result in long-term difficulties in achieving success.

Confidential is that classification of information of which unauthorised disclosure/ use could cause serious damage to the organisation, e.g. strategic planning documents.

Restricted is that classification of information of which unauthorised disclosure/ use would not be in the best interest of the organisation and/or its customers, e.g. design details, computer software (programs, utilities), documentation, organisation personnel data, budget information.

Internal use is that classification of information that does not require any degree of protection against disclosure within the company, e.g. operating procedures, policies and standards inter office memorandums.

Unclassified is that classification of information that requires no protection against disclosure e.g. published annual reports, periodicals. While the above classifications are appropriate for a general organisation viewpoint, the following classifications may be considered:

Top Secret: It shall be applied to information unauthorised disclosure of which could be expected to cause exceptionally grave damage to the national security or national interest. This category is reserved for Nation's closest secrets and to be used with great reserve.

Secret: This shall be applied to information unauthorised disclosure of which could be expected to cause serious damage to the national security or national interest or cause serious embarrassment in its functioning. This classification should be used for highly important information and is the highest classification normally used.

Confidentiality: This shall be applied to information unauthorised disclosure of which could be expected to cause damage to the security of the organisation or could be prejudicial to the interest of the organisation, or could affect the organisation in its

functioning. Most information will on proper analysis be classified no higher than confidential.

Restricted: This shall be applied to information which is essentially meant for official use only and which would not be published or communicated to anyone except for official purpose.

Unclassified: This is the classification of information that requires no protection against disclosure.

4. Physical and Operational Security

4.1 Site Location

(1) Licensed and approved CAs shall have their technical infrastructure in Mauritius.

4.2 Site Design

(1) The site shall not be in locations that are prone to natural or man-made disasters, like flood, fire, chemical contamination and explosions.

(2) As per nature of the operations, suitable floor structuring, lighting, power and water damage protection requirements shall be provided.

(3) Construction shall comply with all applicable building and safety regulations as laid down by the relevant Government agencies. Further, the construction must be tamper-evident.

(4) Materials used for the construction of the operational site shall be fire-resistant and free of toxic chemicals.

(5) External walls shall be constructed of brick or reinforced concrete of sufficient thickness to resist forcible attack. Ground level windows shall be fortified with study mild steel grills or impact-resistant laminated security glass. All internal walls must be from the floor to the ceiling and must be tamper-evident.

(6) Air-conditioning system, power supply system and uninterrupted power supply unit with proper backup shall be installed depending upon the nature of operation. All ducting holes of the air-conditioning system must be designed so as to prevent intrusion of any kind.

(7) Automatic fire detection, fire suppression systems and equipment in compliance with requirement specified under the Occupational Safety and Health Act 2005 or any other agencies of the Government shall be installed at the operational site.

(8) Media library, electrical and mechanical control rooms shall be housed in separate isolated areas, with access granted only to specific, named individuals on a need basis.

(9) Any facility that supports mission-critical and sensitive applications must be located and designed for repairability, relocation and reconfiguration. The ability to relocate, reconstitute and reconfigure these applications must be tested as part of the business continuity/disaster recovery plan.

4.3 **Fire Protection**

(1) Combustible materials shall not be stored within hundred meters of the operational site.

(2) Automatic fire detection, fire suppression systems and audible alarms as prescribed by the Occupational Safety and Health Act 2005 or any other agency of the Government shall be installed at the operational site

(3) Fire extinguishers shall be installed at the operational site and their locations clearly marked with appropriate signs.

(4) Periodic testing, inspection and maintenance of the fire equipment and fire suppression systems shall be carried out.

(5) Procedures for the safe evacuation of personnel in an emergency shall be visibly displayed at prominent places at the operational site. Periodic training and fire drills shall be conducted.

(6) There shall be no eating, drinking or smoking in the operational site. The work areas shall be kept clean at all times.

4.4 Environmental Protection

(1) Water detectors shall be installed under the raised floors throughout the operational site and shall be connected to audible alarms.

(2) The temperature and humidity condition in the operational site shall be monitored and controlled periodically.

(3) Personnel at the operational site shall be trained to monitor and control the various equipment and devices installed at the operational site for the purpose of fire and environment protection.

(4) Periodic inspection, testing and maintenance of the equipment and systems shall be scheduled.

4.5 Physical Access

(1) Responsibilities round the clock, seven days a week, three hundred sixty five days a year for physical security of the systems used for operation and also actual physical layout at the site of operation shall be defined and assigned to named individuals.

(2) Biometric physical access security systems shall be installed to control and audit access to the operational site.

(3) Physical access to the operational site at all times shall be controlled and restricted to authorised personnel only. Personnel authorised for limited physical access shall not be allowed to gain unauthorised access to restricted area within operational site.

(4) Dual control over the inventory and issue of access cards/keys during normal business hours to the Data Centre shall be in place. An up-to-date list of personnel who possess the cards/keys shall be regularly maintained and archived for a period of three years.

(5) Loss of access cards/keys must be immediately reported to the security supervisor of the operational site who shall take appropriate action to prevent unauthorised access.

(6) All individuals, other than operations staff, shall sign in and sign out of the operational site and shall be accompanied by operations staff.

(7) Emergency exits shall be tested periodically to ensure that the access security systems are operational.

(8) All opening of the Data Centre should be monitored round the clock by surveillance video cameras.

5. Information Management

5.1 System Administration

(1) Each organisation shall designate a properly trained "System Administrator" who will ensure that the protective security measures of the system are functional and who will maintain its security posture. Depending upon the complexity and security needs of a system or application, the System Administrator may have a designated System Security Administrator who will assume security responsibilities and provide physical, logical and procedural safeguards for information.

(2) Organisations shall ensure that only a properly trained System Security Administrator is assigned the system security responsibilities.

(3) The responsibility to create, classify, retrieve, modify, delete or archive information must rest only with the System Administrator.

(4) Any password used for the system administration and operation of trusted services must not be written down (in paper or electronic form) or shared with any one. A system for password management should be put in place to cover the eventualities such as forgotten password or changeover to another person in case of System Administrator (or System Security Administrator) leaving the organisation. Every instance of usage of administrator's passwords must be documented.

(5) Periodic review of the access rights of all users must be performed.

(6) The System Administrator must promptly disable access to a user's account if the user is identified as having left the Data Centre, changed assignments, or is no longer requiring system access. Reactivation of the user's account must be authorised in writing by the System Administrator (Digitally signed e-mail may be acceptable).

(7) The System Administrator must take steps to safeguards classified information as prescribed by its owner.

(8) The System Administrator must authorise privileged access to users only on a need-to-know and need-to-do basis and also only after the authorisation is documented.

(9) Criteria for the review of audit trails/access logs, reporting of access violations and procedures to ensure timely management action/response shall be established and documented.

(10) All security violations must be recorded, investigated, and periodic status reports compiled for review by the management.

(11) The System Administrator together with the system support staff, shall conduct a regular analysis of problems reported to and identify any weaknesses in protection of the information.

(12) The System Administrator shall ensure that the data, file and Public Key Infrastructure (PKI) servers are not left unmonitored while these systems are powered on.

(13) The System Administrator should ensure that no generic user is enabled or active on the system.

5.2 **Sensitive Information Control**

(1) Information assets shall be classified and protected according to their sensitivity and criticality to the organisation.

(2) Procedures in accordance with para 8.3 of these Directives must be in place to handle the storage media, which has sensitive and classified information.

(3) All sensitive information stored in any media shall bear or be assigned an appropriate security classification.

(4) All sensitive material shall be stamped or labelled accordingly.

(5) Storage media (i.e. floppy diskettes, magnetic tapes, portable hard disks, optical disks, etc.) containing sensitive information shall be secured according to their classification.

(6) Electronic communication systems, such as router, switches, network device and computers, used for transmission of sensitive information should be equipped or installed with suitable security software and if necessary with an encryptor or encryption software. The appropriate procedure in this regard should be documented.

(7) Procedures shall be in place to ensure the secure disposal of sensitive information assets on all corrupted/damaged or affected media both internal (e.g. hard disk/optical disk) and external (e.g. diskette, disk drive, tapes etc.) to the system. Preferably such affected/corrupted/damaged media both internal and external to the system shall be destroyed.

5.3 **Sensitive Information Security**

(1) Highly sensitive information assets shall be stored on secure removable media and should be in an encrypted format to avoid compromise by unauthorised persons.

(2) Highly sensitive information shall be classified in accordance with para 3.

(3) Sensitive information and data, which are stored on the fixed disk of a computer shared by more than one person, must be protected by access control software (e.g., password). Security packages must be installed which partition or provide authorisation to segregated directories/files.

(4) Removable electronic storage media must be removed from the computer and properly secured at the end of the work session or workday.

(5) Removable electronic storage media containing sensitive information and data must be clearly labelled and secured.

(6) Hard disks containing sensitive information and data must be securely erased prior to giving the computer system to another internal or external department or for maintenance.

5.4 **Third Party Access**

(1) Access to the computer systems by other organisations shall be subjected to a similar level of security protection and controls as in these Information Technology Security Directives.

(2) In case the Data Centre uses the facilities of external service/facility provider (outsourcer) for any of their operations, the use of external service/facility providers (e.g. outsourcer) shall be evaluated in light of the possible security exposures and risks involved and all such agreements shall be approved by the information asset owner. The external service or facility provider shall also sign non-disclosure agreements with the management of the Data Centre/operational site.

(3) The external service/facility provider (e.g. outsourcer) shall provide an equivalent level of security controls as required by these Information Technology Security Directives.

5.5 **Prevention of Computer Misuse**

(1) Prevention, detection, and deterrence measures shall be implemented to safeguard the security of computers and computer information from misuse. The measures taken shall be properly documented and reviewed regularly.

(2) Each organisation shall provide adequate information to all persons, including management, systems developers and programmers, end-users, and third party users warning them against misuse of computers.

(3) Effective measures to deal expeditiously with breaches of security shall be established within each organisation. Such measures shall include:

(i) Prompt reporting of suspected breach;

(ii) Proper investigation and assessment of the nature of suspected breach;

(iii) Secure evidence and preserve integrity of such material as relates to the discovery of any breach;

(iv) Remedial measures

(4) All incidents related to breaches shall be reported to the System Administrator or System Security Administrator for appropriate action to prevent future occurrence.

(5) Procedure shall be set-up to establish the nature of any alleged abuse and determine the subsequent action required to be taken to prevent its future occurrence. Such procedures shall include:

(i) The role of the System Administrator, System Security Administrator and management;

(ii) Procedure for investigation;

(iii) Areas for security review; and

(iv) Subsequent follow-up action.

6. System integrity and security measures

6.1 Use of Security Systems or Facilities

(1) Security controls shall be installed and maintained on each computer system or computer node to prevent unauthorised users from gaining entry to the information system and to prevent unauthorised access to data.

(2) Any system software or resource of the computer system should only be accessible after being authenticated by access control system.

6.2 **System Access Control**

(1) Access control software and system software security features shall be implemented to protect resources. Management approval is required to authorise issuance of user identification (ID) and resource privileges.

(2) Access to information system resources like memory, storage devices etc., sensitive utilities and data resources and programme files shall be controlled and restricted based on a "need-to-use" basis with proper segregation of duties.

(3) The access control software or operating system of the computer system shall provide features to restrict access to the system and data resources. The use of common passwords such as "administrator" or "president" or "game" etc. to protect access to the system and data resources represent a security exposure and shall be avoided. All passwords used must be resistant to dictionary attacks.

(4) Appropriate approval for the request to access system resources shall be obtained from the System Administrator. Directives and procedures governing access authorisations shall be developed, documented and implemented.

(5) An Access Control System manual documenting the access granted to different level of users shall be prepared to provide guidance to the System Administrator for grant of access.

(6) Each user shall be assigned a unique user ID. Adequate user education shall be provided to help users in password choice and password protection. Sharing of user IDs shall not be allowed.

(7) Stored passwords shall be encrypted using internationally proven encryption techniques to prevent unauthorised disclosure and modification.

(8) Stored passwords shall be protected by access controls from unauthorised disclosure and modification.

(9) Automatic time-out for terminal inactivity should be implemented.

(10) Audit trail of security-sensitive access and actions taken shall be logged.

(11) All forms of audit trail shall be appropriately protected against unauthorised modification or deletion.

(12) Where a second level access control is implemented through the application system, password controls similar to those implemented for the computer system shall be in place.

(13) Activities of all remote users shall be logged and monitored closely.

(14) The facility to login as another user from one user's login shall be denied. However, the system should prohibit direct login as a trusted user (e.g. root in Unix, administrator in Windows NT or Windows 2000). This means that there must be a user account configured for the trusted administrator. The system requires trusted users to change their effective username to gain access to root and to re-authenticate themselves before requesting access to privileged functions.

(15) The startup and shutdown procedure of the security software must be automated.

(16) Sensitive Operating System files, which are more prone to hackers must be protected against all known attacks using proven tools and techniques. That is to say no user will be able to modify them except with the permission of System Administrator.

6.3 **Password Management**

(1) Certain minimum quality standards for password shall be enforced. The quality level shall be increased progressively. The following control features shall be implemented for passwords:

(i) Minimum of eight characters without leading or trailing blanks;

(ii) Shall be different from the existing password and the two previous ones;

(iii) Shall be changed at least once every ninety days; for sensitive system, password shall be changed at least once every thirty days; and

(iv) Shall not be shared, displayed or printed.

(2) Password retries shall be limited to a maximum of three attempted logons after which the user ID shall then be revoked; for sensitive systems, the number of password retries should be limited to a maximum of two.

(3) Passwords which are easy-to-guess (e.g. user name, birth date, month, standard words etc.) should be avoided.

(4) Initial or reset passwords must be changed by the user upon first use.

(5) Passwords shall always be encrypted in storage to prevent unauthorised disclosure.

(6) All passwords used must be resistant to dictionary attacks and all known password cracking algorithms.

6.4 **Privileged User's Management**

(1) System privileges shall be granted to users only on a need-to-use basis.

(2) Login privileges for highly privileged accounts should be available only from Console and terminals situated within Console room.

(3) An audit trail of activities conducted by highly privileged users shall be maintained for two years and reviewed periodically at least every week by operator who is independent of System Administrator.

(4) Privileged user shall not be allowed to log in to the computer system from remote terminal. The usage of the computer system by the privilege user shall be allowed during a certain time period.

(5) Separate user IDs shall be allowed to the user for performing privileged and normal (non-privileged) activities.

(6) The use of user IDs for emergency use shall be recorded and approved. The passwords shall be reset after use.

6.5 **User's Account Management**

(1) Procedures for user account management shall be established to control access to application systems and data. The procedures shall include the following:

(i) Users shall be authorised by the computer system owner to access the computer services.

(ii) A written statement of access rights shall be given to all users.

(iii) All users shall be required to sign an undertaking to acknowledge that they understand the conditions of access.

(iv) Where access to computer services is administered by service providers, ensure that the service providers do not provide access until the authorisation procedures have been completed. This includes the acknowledgment of receipt of the accounts by the users.

(v) A formal record of all registered users of the computer services shall be maintained.

(vi) Access rights of users who have been transferred, or left the organisation shall be removed immediately.

(vii) A periodic check shall be carried out for redundant user accounts and access rights that are no longer required.

(viii) Ensure that redundant user accounts are not re-issued to another user.

(2) User accounts shall be suspended under the following conditions:

(i) when an individual is on extended leave or inactive use of over thirty days. In case of protected computer system, the limit of thirty days may be reduced to fifteen days by the System Administrator.

(ii) immediately upon the termination of the services of an individual.

(iii) suspended or inactive accounts shall be deleted after a two months period. In case of protected computer systems, the limit of two months may be reduced to one month.

6.6 **Data and Resource Protection**

(1) All information assets shall be assigned an "owner" responsible for the integrity of that data/resource. Custodians shall be assigned and shall be jointly responsible for information assets by providing computer controls to assist owners.

(2) The operating system or security system of the computer system shall:

(i) Define user authority and enforce access control to data within the computer system;

(ii) Be capable of specifying, for each named individual, a list of named data objects (e.g. file, programme) or groups of named objects, and the type of access allowed.

(3) For networked or shared computer systems, system users shall be limited to a profile of data objects required to perform their needed tasks.

(4) Access controls for any data and/or resources shall be determined as part of the systems analysis and design process.

(5) Application Programmer shall not be allowed to access the production system.

7. **Sensitive Systems Protection**

(1) Security tokens/smart cards/bio-metric technologies such as Iris recognition, finger print verification technologies etc. shall be used to complement the usage of passwords to access the computer system.

(2) For computer system processing sensitive data, access by other organisations shall be prohibited or strictly controlled.

(3) For sensitive data, encryption of data in storage shall be considered to protect its confidentiality and integrity.

8. Data Centre Operations Security

8.1 Job Scheduling

(1) Procedures shall be established to ensure that all changes to the job schedules are appropriately approved. The authority to approve changes to job schedules shall be clearly assigned.

(2) As far as possible, automated job scheduling should be used. Manual job scheduling should require prior approval from the competent authority.

8.2 System Operations Procedure

(1) Procedures shall be established to ensure that only authorised and correct job stream and parameter changes are made.

(2) Procedures shall be established to maintain logs of system activities. Such logs shall be reviewed by a competent independent party for indications of dubious activities. Appropriate retention periods shall be set for such logs.

(3) Procedures shall be established to ensure that people other than well-trained computer operators are prohibited from operating the computer equipment.

(4) Procedures shall be implemented to ensure the secure storage or distribution of all outputs/reports, in accordance with procedures defined by the owners for each system.

8.3 Media Management

(1) Responsibilities for media library management and protection shall be clearly defined and assigned.

(2) All media containing sensitive data shall be stored in a locked room or cabinets, which must be fire resistant and free of toxic chemicals.

(3) Access to the media library (both on-site and off-site) shall be restricted to the authorised persons only. A list of personnel authorised to enter the library shall be maintained.

(4) The media containing sensitive and back up data must be stored at three different physical locations in the country, which can be reached in few hours.

(5) A media management system shall be in place to account for all media stored on-site and off-site.

(6) All incoming/outgoing media transfers shall be authorised by management and users.

(7) An independent physical inventory check of all media shall be conducted at least every six months.

(8) All media shall have external volume identification. Internal labels shall be fixed, where available.

(9) Procedures shall be in place to ensure that only authorised addition/removal of media from the library is allowed.

(10) Media retention periods shall be established and approved by management in accordance with legal/regulatory and user requirements.

8.4 **Media Movement**

(1) Proper records of all movements of computer tapes/disks between on-site and off-site media library must be maintained.

(2) There shall be procedures to ensure the authorised and secure transfer to media to/from external parties and the off-site location. A means to authenticate the receipt shall be in place.

(3) Computer media that are being transported to off-site data backup locations should be stored in locked carrying cases that provide magnetic field protection and protection from impact while loading and unloading and during transportation.

9. **Data Backup and Off-site Retention**

(1) Back-up procedures shall be documented, scheduled and monitored.

(2) Up-to-date backups of all critical items shall be maintained to ensure the continued provision of the minimum essential level of service. These items include:

(i) Data files

(ii) Utilities programmes

(iii) Databases

(iv) Operating system software

(v) Applications system software

(vi) Encryption keys

(vii) Pre-printed forms

(viii) Documentation (including a copy of the business continuity plans)

(3) One set of the original disks for all operating system and application software must be maintained to ensure that a valid, virus-free backup exists and is available for use at any time.

(4) Backups of the system, application and data shall be performed on a regular basis. Backups should also be made for application under development and data conversion efforts.

(5) Data backup is required for all systems including personal computers, servers and distributed systems and databases.

(6) Critical system data and file server software must have full backups taken weekly.

(7) The backups must be kept in an area physically separate from the server. If critical system data on the LAN represents unique versions of the information assets, then the information backups must be rotated on a periodic basis to an off-site storage location.

(8) Critical system data and file server software must have incremental backups taken daily.

(9) Systems that are completely static may not require periodic backup, but shall be backed up after changes or updates in the information.

(10) Each LAN/system should have a primary and backup operator to ensure continuity of business operations.

(11) The business recovery plan should be prepared and tested on an annual basis.

10. **Audit Trails and Verification**

(1) Transactions that meet exception criteria shall be completely and accurately highlighted and reviewed by personnel independent of those that initiate the transaction.

(2) Adequate audit trails shall be captured and certain information needed to determine sensitive events and pattern analysis that would indicate possible fraudulent use of the system (e.g. repeated unsuccessful logons, access attempts over a series of days) shall be analysed. This information includes such information as who, what, when, where, and any special information such as:

(i) Success or failure of the event

(ii) Use of authentication keys, where applicable

(3) Automated or manual procedures shall be used to monitor and promptly report all significant security events, such as accesses, which are out-of-pattern relative to time, volume, frequency, type of information asset, and redundancy. Other areas of analysis include:

(i) Significant computer system events (e.g. configuration updates, system crashes)

(ii) Security profile changes

(iii) Actions taken by computer operations, system administrators, system programmers, and/or security administrators

(4) The real time clock of the computer system shall be set accurately to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases.

(5) The real time clock of the computer or communications device shall be set to Mauritian Time. Further there shall be a procedure that checks and corrects drift in the real time clock.

(6) Computer system access records shall be kept for a minimum of ten years, in either hard copy or electronic form. Records, which are of legal nature and necessary for any legal or regulation requirement or investigation of criminal behaviour, shall be retained as per laws of the land.

(7) Computer records of applications transactions and significant events must be retained for a minimum period of ten years or longer depending on specific record retention requirements.

11. **Measures to Handle Computer Virus**

(1) Responsibilities and duties shall be assigned to ensure that all file servers and personal computers are equipped with up-to-date virus protection and detection software.

(2) Virus detection software must be used to check storage drives both internal and external to the system on a periodic basis.

(3) All diskettes and software shall be screened and verified by virus detection software before being loaded onto the computer system. No magnetic media like tape cartridge, floppies etc. brought from outside shall be used on the data, file, PKI or

computer server or personal computer on Intranet and Internet without proper screening and verification by virus detection software.

(4) A team shall be designated to deal with reported or suspected incidents of computer virus. The designated team shall ensure that latest version of anti-virus software is loaded on all data, file, PKI servers and personal computers.

(5) Procedures shall be established to limit the spread of viruses to other organisation information assets. Such procedures inter alia shall include:

(i) Communication to other business partners and users who may be at risk from an infected resource

(ii) Eradication and recovery procedures

(iii) Incident report must be documented and communicated per established procedures.

(6) An awareness and training programme shall be established to communicate virus protection practices, available controls, areas of high risk to virus infection and responsibilities.

12. **Relocation of Hardware and Software**

Whenever computers or computer peripherals are relocated (e.g. for maintenance, installation at different sites or storage), the following directives shall apply:

(i) All removable media will be removed from the computer system and kept at secure location.

(ii) Internal drives will be overwritten, reformatted or removed as the situation may be.

(iii) If applicable, ribbons will be removed from printers.

(iv) All paper will be removed from printers.

13. **Hardware and Software Maintenance**

Whenever, the hardware and software maintenance of the computer or computer network is being carried out, the following should be considered:

(1) Proper placement and installation of Information Technology equipment to reduce the effects of interference due to electromagnetic emanations.

(2) Maintenance of an inventory and configuration chart of hardware.

(3) Identification and use of security features implemented within hardware.

(4) Authorisation, documentation, and control of change made to the hardware.

(5) Identification of support facilities including power and air conditioning.

(6) Provision of an uninterruptible power supply.

(7) Maintenance of equipment and services.

(8) Organisation must make proper arrangements for maintenance of computer hardware, software (both system and application) and firmware installed and used by them. It shall be the responsibility of the officer in charge of the operational site to ensure that contract for annual maintenance of hardware is always in place.

(9) Organisation must enter into maintenance agreements, if necessary, with the supplier of computer and communication hardware, software (both system and application) and firmware.

(10) Maintenance personnel will sign non-disclosure agreements.

(11) The identities of all hardware and software vendor maintenance staff should be verified before allowing them to carry out maintenance work.

(12) All maintenance personnel should be escorted within the operational site/computer system and network installation room by the authorised personnel of the organisation.

(13) After maintenance, any exposed security parameters such as passwords, user IDs, and accounts will be changed or reset to eliminate any potential security exposures.

(14) If the computer system, computer network or any of its devices is vulnerable to computer viruses as a result of performing maintenance, system managers or users shall scan the computer system and its devices and any media affected for viruses as a result of maintenance.

14. **Purchase and Licensing of Hardware and Software**

(1) Hardware and software products that contain or are to be used to enforce security, and intended for use or interface into any organisation system or network, must be verified to comply with these Information Technology Security Directives prior to the signing of any contract, purchase or lease.

(2) Software, which is capable of bypassing or modifying the security system or operating system, integrity features, must be verified to determine that they conform to these Information Technology Security Directives. Where such compliance is not possible, then procedures shall be in place to ensure that the implementation and operation of that software does not compromise the security of the system.

(3) There shall be procedures to identify, select, implement and control software (system and application software) acquisition and installation to ensure compliance with the Mauritian Copyright Act and Information Technology Security Directives.

(4) It is prohibited to knowingly install on any system whether test or production, any software which is not licensed for use on the specific systems or networks.

(5) No software will be installed and used on the system when appropriate licensing agreements do not exist, except during evaluation periods for which the user has documented permission to install and test the software under evaluation.

(6) Illegally acquired or unauthorised software must not be used on any computer, computer network or data communication equipment. In the event that any illegally acquired or unauthorised software is detected by the System Administrator or Network Administrator, the same must be removed immediately.

15. **System Software**

(1) All system software options and parameters shall be reviewed and approved by the management.

(2) System software shall be comprehensively tested and its security functionality validated prior to implementation.

(3) All vendor supplied default user IDs shall be deleted or password changed before allowing users to access the computer system.

(4) Versions of system software installed on the computer system and communication devices shall be regularly updated.

(5) All changes proposed in the system software must be appropriately justified and approved by an authorised party.

(6) A log of all changes to system software shall be maintained, completely documented and tested to ensure the desired results.

(7) Procedures to control changes initiated by vendors shall be in accordance with para 21 pertaining to "Change Management".

(8) There shall be no standing "Write" access to the system libraries. All "Write" access shall be logged and reviewed by the System Administrator for dubious activities.

(9) System Programmers shall not be allowed to have access to the application system's data and programme files in the production environment.

(10) Procedures to control the use of sensitive system utilities and system programmes that could bypass intended security controls shall be in place and documented. All usage shall be logged and reviewed by the System Administrator and another person independent of System Administrator for dubious activities.

16. **Documentation Security**

(1) All documentation pertaining to application software and sensitive system software and changes made therein shall be updated to the current time, accurately and stored securely. An up-to-date inventory list of all documentation shall be maintained to ensure control and accountability.

(2) All documentation and subsequent changes shall be reviewed and approved by an independent authorised party prior to issue.

(3) Access to application software documentation and sensitive system software documentation shall be restricted to authorised personnel on a "need-to-use" basis only.

(4) Adequate backups of all documentation shall be maintained and a copy of all critical documentation and manuals shall be stored off-site.

(5) Documentation shall be classified according to the sensitivity of its contents/implications.

(6) Organisations shall adopt a clean desk policy for papers, diskettes and other documentation in order to reduce the risks of unauthorised access, loss of and damage to information outside normal working hours.

17. **Network Communication Security**

(1) All sensitive information on the network shall be protected by using appropriate techniques. The critical network devices such as routers, switches and modems should be protected from physical damage.

(2) The network configuration and inventories shall be documented and maintained.

(3) Prior authorisation of the Network Administrator shall be obtained for making any changes to network configuration. The changes made in the network configuration shall be documented. The threat and risk assessment of the network after changes in the network configuration shall be reviewed. The network operation shall be monitored for any security irregularity. A formal procedure should be in place for identifying and resolving security problems.

(4) Physical access to communications and network sites shall be controlled and restricted to authorised individuals only in accordance with para 4.5 pertaining to "Physical Access".

(5) Communication and network systems shall be controlled and restricted to authorised individuals only in accordance with para 6.2 – System Access Control.

(6) As far as possible, transmission medium within the Certification Authority's operational site should be secured against electro magnetic transmission. In this regard, use of Optical Fibre Cable and armoured cable may be preferred as transmission media as the case may be.

(7) Network diagnostic tools, e.g., spectrum analyzer, protocol analyzer should be used on a need basis.

18. **Firewalls**

(1) Intelligent devices generally known as "Firewalls" shall be used to isolate organisation's data network with the external network. Firewall device should also be used to limit network connectivity for unauthorised use.

(2) Networks that operate at varying security levels shall be isolated from each other by appropriate firewalls. The internal network of the organisation shall be physically and logically isolated from the Internet and any other external connection by a firewall.

(3) All firewalls shall be subjected to thorough test for vulnerability prior to being put to use and at least half-yearly thereafter.

(4) All web servers for access by Internet users shall be isolated from other data and host servers.

19. **Connectivity**

(1) Organisation shall establish procedure for allowing connectivity of their computer network or computer system to non-organisation computer system or networks. The permission to connect other networks and computer system shall be approved by the Network Administrator and documented.

(2) All unused connections and network segments should be disconnected from active networks. The computer system/personal computer or outside terminal accessing an organisation's host system must adhere to the general system security and access control directives.

(3) The suitability of new hardware/software particularly the protocol compatibility should be assessed before connecting the same to the organisation's network.

(4) As far as possible, no Internet access should be allowed to database server/file server or server hosting sensitive data.

(5) The level of protection for communication and network resources should be commensurate with the criticality and sensitivity of the data transmitted.

20. **Network Administrator**

(1) Each organisation shall designate a properly trained "Network Administrator" who will be responsible for operation, monitoring security and functioning of the network.

(2) Network Administrator shall regularly undertake the review of network and also take adequate measures to provide physical, logical and procedural safeguards for its security. Appropriate follow up of any unusual activity or pattern of access on the computer network shall be investigated promptly by the Network Administrator.

(3) System must include a mechanism for alerting the Network Administrator of possible breaches in security, e.g., unauthorised access, virus infection and hacking.

(4) Secure Network Management System should be implemented to monitor functioning of the computer network. Broadcast of network traffic should be minimised.

(5) Only authorised and legal software shall be used on the network.

(6) Shared computer systems, network devices used for business applications shall comply with the requirement established in para 6 – System Integrity and Security Measures.

21. Change Management

21.1 Change Control

(1) Procedures for tracking and managing changes in application software, system software, hardware and data in the production system shall be established. Organisational responsibilities for the change management process shall be defined and assigned.

(2) A risk and impact analysis, classification and prioritisation process shall be established.

(3) No changes to a production system shall be implemented until such changes have been formally authorised. Authorisation procedures for change control shall be defined and documented.

(4) Owners/Users shall be notified of all changes made to production system which may affect the processing of information on the said production system.

(5) Fall-back procedures in the event of a failure in the implementation of the change process shall be established and documented.

(6) Procedures to protect, control access and changes to production source code, data, execution statements and relevant system documentation shall be documented and implemented.

(7) Version changes of application software and all system software installed on the computer systems and all communication devices shall be documented. Different versions of application software and system software must be kept in safe custody.

21.2 Testing of Changes to Production System

(1) All changes in computer resource proposed in the production system shall be tested and the test results shall be reviewed and accepted by all concerned parties prior to implementation.

(2) All user acceptance tests in respect of changes in computer resource in production system shall be performed in a controlled environment which includes: (i) Test objectives, (ii) A documented test plan, and (iii) acceptance criteria.

21.3 **Review of Changes**

(1) Procedures shall be established for an independent review of programme changes before they are moved into a production environment to detect unauthorised or malicious codes.

(2) Procedures shall be established to schedule and review the implementation of the changes in computer resource in the production system so as to ensure proper functioning.

(3) All emergency changes/fixes in computer resource in the production system shall be reviewed and approved.

(4) Periodic management reports on the status of the changes implemented in the computer resourced in the production system shall be submitted for management review.

22. **Problem Management and Reporting**

(1) Procedures for identifying, reporting and resolving problems, such as non-functioning of Certification Authority's system; breaches in Information Technology security; and hacking, shall be established and communicated to all personnel concerned. It shall include emergency procedures. Periodic reports shall be submitted for management review.

(2) A help desk shall be set up to assist users in the resolution of problems.

(3) A system for recording, tracking and reporting the status of reported problems shall be established to ensure that they are promptly managed and resolved with minimal impact on the user of the computing resources.

23. **Emergency Preparedness**

(1) Emergency response procedures for all activities connected with computer operation shall be developed and documented. These procedures should be reviewed periodically.

(2) Emergency drills should be held periodically to ensure that the documented emergency procedures are effective.

24. **Contingency Recovery Equipment and Services**

(1) Commitment shall be obtained in writing from computer equipment and supplies vendors to replace critical equipment and supplies within a specified period of time following a destruction of the computing facility.

(2) The business continuity plan shall be developed which inter alia include the procedures for emergency ordering of the equipment and availability of the services.

(3) The need for backup hardware and other peripherals should be evaluated in accordance to business needs.

25. **Security Incident Reporting and Response**

(1) All security related incidents must be reported to central coordinator or equivalent, appointed by the management to coordinate and handle security related incidents. This central coordinator shall be the single point of contact at the organisation.

(2) All incidents reported, actions taken, follow-up actions, and other related information shall be documented.

(3) Procedures shall be defined for dealing with all security related incidents, including malicious software, break-ins from networks, software bugs which compromised the security of the system.

26. **Disaster Recovery/Management**

(1) Disaster recovery plan shall be developed, properly documented, tested and maintained to ensure that in the event of a failure of the information system or destruction of the facility, essential level of service will be provided. The disaster recovery framework should include:

(a) emergency procedures, describing the immediate action to be taken in case of a major incident

(b) fall back procedure, describing the actions to be taken to relocate essential activities or support services to a backup site

(c) restoration procedures, describing the action to be taken to return to normal operation at the original site.

(2) The documentation should include:

(a) definition of a disaster;

(b) condition for activating the plan;

(c) stages of a crisis;

(d) who will make decisions in the crisis;

(e) role of individuals for each component of the plan;

(f) composition of the recovery team; and

(g) decision making process for return to normal operation.

(3) Specific disaster management plan for critical applications shall be developed, documented, tested and maintained on a regular basis.

(4) Responsibilities and reporting structure shall be clearly defined which will take effect immediately on the declaration of a disaster.

(5) Each component/aspect of the plan should have a person and a backup assigned to its execution.

(6) Periodic training of personnel and users associated with computer system and network should be conducted defining their roles and responsibilities in the event of a disaster.

(7) Test plan shall be developed, documented and maintained. Periodic tests shall be carried out to test the effectiveness of the procedures in the plan. The results of the tests shall be documented for management review.

(8) Disaster recovery plan should be updated regularly to ensure its continuing effectiveness.