REPUBLIC OF KENYA

ICT SECURITY POLICY

BY

MINISTRY OF INFORMATION & COMMUNICATIONS

MARCH 2010

TABLE OF CONTENTS

1. INTRODUCTION

These guidelines are for the implementation and management of ICT security. Due to the rapid changes in information and communication technology some aspects of the guidelines may not apply in some organizations. It is the responsibility of organizations to develop internal security processes that meet the general guidelines set forth in this document.

The following words used in the ICT Security guidelines shall be interpreted as follows:

Shall: a mandatory requirement, and therefore must be complied with.

Should: a recommended requirement. Non-compliance shall be documented and approved by management.

Must: the guidelines defined are mandatory and therefore must be complied with.

May: the guidelines defined are optional. Its implementation is determined by the organization's requirement.

2. IMPLEMENTATION OF AN INFORMATION SECURITY PROGRAMME

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 the Information Classification System

(d) Development and Implementation of security standards manual

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

(f) On-going security programme maintenance and enforcement

(g) Training

3. INFORMATION CLASSIFICATION

(1) Information assets must be classified according to the importance and sensitivity to the organisation. Classification, declassification, labeling, storage, access, destruction and reproduction of classified data and the administrative overhead this process creates must be addressed. Organisations should consider the following classification of automated information:

(a) Confidential: Classification of information which unauthorized disclosure/use could cause damage to the organisation, e.g. strategic planning documents.

(b) Restricted: Classification of information in which unauthorized disclosure/use would no be in the best interest of the organisation and or its customers, e.g. design details, computer software, documentation, personnel data, budget information etc.

(c) Internal use: classification of information that does not require any degree of protection against disclosure within the organisation, e.g. operating procedures, policies, and internal memos.

(d) Unclassified: Classification of information requires no protection against disclosure, e.g. published annual reports, periodicals, etc

(2) The following additional classification may be considered:

(a) Top Secret: It shall be applied to information to which unauthorized disclosure can cause exceptionally grave damage to national security or national interest. This category is reserved for the nation's closest secrets and must be used in great reservation.

(b) Secret: Classification of information whose unauthorized disclosure can cause serious damage to national security or national interest or cause serious embarrassment. This classification is used for highly important information and is the highest classification normally used.

(c) Confidential:Classification of information whose unauthorized disclosure could be expected to cause damage to the security of the organisation or could be prejudicial the interests of the organisation, or could affect the organisation in its functioning.

(d) Restricted: This is meant for information which is essentially meant for official use only and which could not be published or mmunicated to anyone except for official purpose.

(e) Unclassified:This is information that requires no protection against disclosure.

4. PHYSICAL AND OPERATIONAL SECURITY

(1) Site Design

(a) The site shall be located in a secure environment not fire, chemical contamination or explosions

(b) As per the nature of operations, suitable floor struct lighting, power and water damage protection shall be provided

(c) Construction shall comply with building and safety regulations as laid down by the relevant government ministry.

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

(e) Externals walls shall be constructed from brick or reinforced concrete of sufficient thickness to resist forcible attack. Ground level windows shall be fortified with sturdy mild steel grills or impact resistant laminated security glass. All internal walls must be from floor to ceiling and must be temper evident.

(f) Air conditioning system, power supply system and uninterrupted power supply units with proper back-up shall be installed depending on the nature of the operation. All ducting holes of the air conditioning system must be designed so as to prevent intrusion of any kind.

(g) For large and protected installations, the 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.

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

(2) Fire Protection

(a) Combustible materials shall not be stored within one hundred metres of the operational site.

(b) Automatic fire detection system, fire suppression systems shall be installed in compliance with the requirements specified by the Ministry of Public Works shall be installed at the operational site.

(c) Fire extinguishers shall be installed at the operational site and their locations clearly marked.

(d) Periodic testing, inspection and maintenance of fire equipment and fire suppressing systems shall be carried out.

(e) Procedures for safe evacuation of personnel in an emergency shall be displayed at prominent places at the operational site.

(f) Periodic training and fire drills shall be conducted.

(g) There shall be no eating, drinking or smoking in the operational site.

(h) Work areas shall be kept clean at all times.

(3) Fire Protection

(a) The responsibility for a 24-hour, seven days a week, three hundred and sixty five days a year for the physical security of the used for operation and also actual physical layout at the site operation shall be defined and assigned to an individual.

(b) A biometric physical assess security system shall be installed at all high security installations to control and audit access to the operational site.

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

(d) Dual control over the inventory and issue of access keys or cards during normal business hours at the data centre shall be in place. An up-to-date list of personnel who posses the keys or cards shall be regularly maintained and archived for a period of three years.

(e) 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.

(f) All individuals other that operational staff shall sig in and out of the operational site and shall be accompanied by operational staff.

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

(h) All entrances to the data centre must be monitored round the clock by surveillance video cameras.

(4) Environmental Protection

(a) Water detectors shall be installed under raised floors throughout the operation sites and shall be connected to audible alarms.

(b) The temperature and humidity of the operation site shall be monitored and controlled periodically.

(c) Personnel at the operations site shall be trained to monitor and control the various fire and environmental protection equipment and devices installed at the site.

(d) Periodic inspection, testing and maintenance of the fire and environmental protection equipment and systems shall be carried out.

5. INFORMATION MANAGEMENT

(1) Systems Administration

(a) Each organisation shall designate a properly trained "systems administrator" who will ensure that the protective security measures of the system are functional and who will maintain the securi system. Depending upon the complexity and security needs of the system, systems administrator may have a designated properly trained systems security administrator who will provide physical, logical and procedural safeguards for information.

(b) The responsibility to create, retrieve, modify, delete or archive information must rest with the system administrator.

(c) Any passwords used by the systems administrator for the administration and operation of trusted devices must not be written down (in paper or electronic form) or shared with anyone. A system for password management should be put in place to cover possible eventualities such as forgotten passwords or changeover to another person in case the s administrator (or systems security administrator) leaving the organisation.

(d) Periodic reviews of access rights of all users must be performed.

(e) The systems administrator must promptly disable access to a user's account if the user is identified as having left the organisation or changed assignments, or is not longer required to have systems access. The systems administrator must authorize re-activation of the user's account in writing. A digitally signed e-mail may be acceptable).

(f) The systems administrator must take steps to safeguard classified information as prescribed by the owner.

(g) The systems administrator must authorize in writing privileged access to users irrespective of their seniority on need-to-know or need-to-do basis.

(h) The criteria for review of audit of audit trails, access logs, reporting of access violations and procedures to ensure timely management shall be established and documented.

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

(j) The systems administrator together with the systems support staff shall conduct regular analysis of problems reported to identify weaknesses in the protection of information.

(k) The systems administrator shall ensure that no generic user is enabled or active on the system.

(2) Sensitive Information Control

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

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

(c) All sensitive materials shall be stamped and labeled accordingly.

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

(e) Electronic communication systems such as routers, switches, network device and computers, used for transmission of sensitive information should be equipped or with suitable security software and if y with encryption or decryption software.

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

(3) Sensitive Information Security

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

(b) Highly sensitive information shall be classified according to paragraph 3.

(c) Sensitive information which is stored on fixed disks of a computer shored by more than one person must be protected by access control software (e.g. password). Security packages must be installed which partition or provide authorization to segregated directories/files.

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

(e) Removable electronic storage media containing sensitive information must be clearly labeled and secured.

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

(4) Third Party Access

(a) Access to the computer systems by other organisation shall be subjected to a similar level of security protection as these information security guidelines.

(b) In case the Data Centre outsources any of its operations, the use of such services shall be evaluated in the light of possible security exposures and risks involved. The information asset owner shall approve all such agreements. The external service/facility providers must sign a non-disclosure agreement with the management of the Data Centre/operational site.

(c) The external service/facility provider shall provide an equivalent level of security controls as required by these information technology guidelines.

(5) Prevention of Computer Misuse

(a) Prevention, detection and deterrence measures shall be implemented to safeguard security of computers and computer informati from misuse. The measures shall be properly documented and reviewed.
(b) Each organisation shall provide adequate information to all persons, including management, systems developers, programmers third party users warning them against computer misuse.
(c) Effective measure to deal expeditiously with breaches security shall be established within each organisation. Such measures shall include:

(i) Prompt reporting of security incidences;

(ii) Prompt investigation and assessment of the nature of the selected breach;

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

(iv) Take remedial measures as necessary.

(d) All incidences related to breaches shall be reported to the Systems Administrator or Systems Security Administrator for appropriate action to prevent future occurrences;

(e) Procedures shall be set up to establish the nature of alleged abuse and to determine subsequent action required to be taken to prevent its future occurrence. Such procedures shall provide:

(i) the role of the systems administrator, systems security administrator and management;

(ii) Procedure for investigation;

(iii) Areas for security review; and

(iv) Subsequent follow-up action.

6. SYSTEMS INTEGRITY AND SECURITY MEASURES

(1) Use of Security Systems or Facilities

(a) Security Controls shall be installed and maintained on each computer system or computer node to prevent unauthorized users gaining entry to the information system and to prevent unauthorized access to data

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

(2) Systems Access Control

(a) Access control software and systems software security features shall be implemented to protect resources. Management approval required to authorize issuance of user identification Ids and resource access privileges.

(b) 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.

(c) The access software or operating system of the computer system shall provide features to restrict access to the system and data All passwords used must be resistant to dictionary attack.

(d) Appropriate approval for the request to access system shall be obtained from the systems administrator. Guidelines and procedures governing access authorization shall be developed, documented and implemented.

(e) An access control systems manual documenting the access granted to different level of users shall be prepared to provide idance to the systems administrator for grant of access.

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

(g) Stored passwords shall be encrypted using international encryption standards to prevent unauthorised disclosure and modification.

(h) Stored pass words shall be protected by access controls from unauthorised disclosure and modification.

(i) Automatic time-out shall be implemented during terminal inactivity.

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

(k) All forms of audit trail shall be appropriately protected against unauthorised modification.

(l) Where second level accesses control is implemented through the application system, password controls similar to those implemented for the operating system shall be in place.

(m) Activities of all remote users shall be monitored and logged at all times.

(n) The facility to login as another user from one user's login shall be denied.

(o) The start-up and shutdown procedure of the security software must be automated.

(p) Sensitive operating system files, which are more prone to hackers, must be protected against all known attacks using proven tools and techniques.

(3) Password Management

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

(a) Minimum of eight characters without leading or training blanks;

(b) Each new password shall be different from the previous three passwords;

(c) Each password shall be changed once every 90 days. However, for sensitive systems, password shall be changed at least every thirty days; and

(d) Passwords shall not be shared, displayed or printed.

(2) Password entries shall be limited to a maximum of three attempted logons after which the user ID shall be revoked; for sensitive systems, the number of passwords 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) The user upon first use must change initial or rest passwords.

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

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

(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 consoles and terminals within the computer room.

(3) An audit trail of activities conducted by highly privileged users shall be maintained for two years and reviewed periodically by operator who is independent of the systems administrator.

(4) Privileged users shall not be allowed to log in to the computer system from a remote terminal.

(5) The usage of the computer system by a privileged user be allowed during a certain time period only.

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

(7) The use of user Ids for emergency purpose shall be recorded and approved. The passwords shall be rest after use.

(5) User Account Management

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

(a) Users shall be authorized by the computer system owner to access computer services;

(b) A written statement of access rights shall be given to all users;

(c) All users shall be required to sign an undertaking to acknowledge that they understand the access conditions;

(d) Where access to computer service is administered by service providers, ensure that the service providers do not provide access until the authorization procedures have been completed. This includes the acknowledgement of receipt of the accounts by users;

(e) A formal record of all registered users of the computer services shall be maintained;

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

(g) A periodic check shall be carried out for redundant user accounts and access rights that are no longer required. Such accounts shall not be re-issued to another user;

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

(i) when an individual is on extended leave or the account is for thirty days. In the case of protected computer system, the limit of thirty days may be reduced to fifteen days; and

(ii) Immediately after the termination of services of an employee;

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

(6) Data and Resource Protection

(a) All information shall be assigned to an "owner" responsible for the integrity of the information resource. Custodians shall be assig and shall be responsible for the information assets by providing computer controls to assist the owner.

(b) 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, program) or groups of named objects, and the type of access allowed

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

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

(e) Application programmer shall not be allowed to access the production process.

7. SENSITIVE SYSTEMS PROTECTION

(1) Security tokens/smart cards/biometric technologies such as iris recognition, fingerprint verification, etc shall be used to compliment the usage of passwords to access the computer system.

(2) Access by other organisations shall be prohibited or strictly controlled for computer systems processing sensitive.

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

8. DATA CENTRE OPERATIONS SECURITY

(1) Job Scheduling

(a) Procedures shall be established to ensure that all changes to the job schedules are appropriately approved.

(b) The authority to approve changes to job schedules shall be clearly defined.

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

(2) Systems Operations Procedure

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

(b) Procedures shall be established to maintain logs of system activities. Such logs should be reviewed by competent parties for indications of dubious activities. Appropriate retention periods shall be set for such logs.

(c) Procedures shall be established to ensure that no persons other than well-trained computer operators are allowed to operate the computer equipment.

(d) Procedures shall be implemented to ensure that the security storage or distribution of all output/reports is carried out in accordance with procedures defined by the owners of the system.

(3) Media Management

(a) Responsibility for media library management and protection shall be clearly defined and assigned.

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

(c) Access to the media library (both onsite and off-site) shall be restricted to the authorized persons only. A list of persons authorized to enter the library shall be maintained.

(d) The media containing sensitive and back-up data must be stored at three different physical locations, which can be reached within a few hours.

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

(f) All incoming and outgoing media transfers shall be authorized by management and users.

(g) An independent physical inventory check shall be conducted at least every six months.

(h) All media shall have external volume identification.

(i) Procedures shall be in place to ensure that only authorized additions/removals of media from the library is allowed.

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

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

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

(m) Computer media being transported to and from back-up sites should be locked in carrying cases that provide both magnetic protection and protection from impact.

9. BACK UP AND OFF-SITE RETENTION

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

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

(a) Data files

(b) Utilities programs

(c) Databases

(d) Operating system software

(e) Application system software

(f) Encryption keys

(g) Pre-printed forms

(h) Documentation (including the business continuity plans)

(3) One set of the original disks for the 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) Backup of the system, application and data shall be performed on regular basis.

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

(6) Critical system data and file server software must have full backup taken daily for critical systems and weekly for other systems.

(7) The backup must be kept in an area physically separate from the server. If critical system data on the Local Area Network 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) Systems that are completely static may not require bac but shall be backed up after changes or updates to the information.

(9) Business recovery plan should be prepared and tested on an annual basis.

10. AUDIT TRAILS AND VERIFICATION

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

(2) Adequate trail shall be captured and certain information needed to determine sensitive events and pattern analysis that indicate possible fraudulent use of the system (e.g. repeated unsuccessful logons, access attempts over a series of days) shall be analyzed. This information includes such information as who, what, where, and any special such as success or failure of event and use of authentication keys.

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

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

(5) The real time clock of the computer system shall be set to the standard East African Time. Further, there shall be a procedure established to check and correct drift in the real time clock.

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

11. MEASURE TO HANDLE COMPUTER VIRUSES

(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 periodic basis.

(3) All removable media and software shall be screened and verified by virus detection software before being loaded onto the computer system.

(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 resources. Such procedures shall inter alia include:

(a) Communication to other business partners and users who may be at risk from an infected source;

(b) Setting up eradication and recovery procedures

(c) Setting up procedures for documenting and communicating incidence reports.

(6) All users shall be trained on virus protection practices, available controls, areas of high risk and responsibilities.

12. RELOCATION OF COMPUTER HARDWARE AND SOFTWARE

Whenever computers or computer peripherals are relocated (e.g. for maintenance, re-installation or storage), the following guidelines shall apply:

(1) All removable media will be removed from the computer and kept in a secure location.

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

(3) All paper and ribbons shall be removed from printers.

13. COMPUTER HARDWARE AND SOFTWARE MAINTENANCE

Whenever, the hardware and software maintenance if a 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 chances of damage from electromagnetic interference.

(2) An inventory and configuration chart of the hardware be maintained

(3) All changes to the hardware and the security features built in it must be authorized and documented.

(4) Maintenance personnel for sensitive systems must sign non-disclosure agreement.

(5) Identities of all hardware and software vendor maintenance staff should be verified before they are allowed to carry out the maintenance work.

(6) For sensitive systems, authorized personnel of the organisation should escort all maintenance personnel within the operational site/computer system site.

(7) After maintenance, any exposed security parameters such as passwords, user Ids, and user accounts must be changed or reset to eliminate potential security exposure.

(8) If a computer system, computer network or computer peripheral is vulnerable to computer viruses as a result of performing maintenance, the systems administrators and users shall scan the computer system, its peripherals and any media affected for viruses as a result of maintenance activities.

14. PURCHASE AND LICENSING OF HARDWARE AND SOFTWARE

(1) Hardware and software products that are to be used enforce security and intended for use or interface into any organisation system or network, must be verified to comply with these information technology security guidelines prior to signing any contract, purchase or lease.

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

(3) There shall be procedures to identify, select, implement and control computer software to ensure compliance with the Copyright Act and Information Technology Security guidelines.

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

(5) No software shall be installed and used on a computer system or computer network when appropriate licencing 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 unauthorized software must not be used on any computer, computer network or data communication equipment. In the event that the systems administrator or network administrator detects any illegally acquired or unauthorized software, the same must be removed immediately.

15. SYSTEMS SOFTWARE

(1) All system software options and parameters shall be reviewed and approved by 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 passwords changed before allowing users to access the computer system.

(4) All changes proposed in the systems software must be appropriately justified and approved by an authorized authority.

(5) A log of all changes to the system software shall be maintained and documented.

(6) There shall be no standing “Write” access to the system libraries on any computer system. All “Write” access shall be logged and reviewed by the systems administrator for dubious activities.

(7) System programmers shall not be allowed to have access to the application system’s data or program files in the production environment.

(8) Procedures to control the use of sensitive system utilities and system programs that could bypass intended security controls shall be in place and documented.

16. SECURITY OF SYSTEM DOCUMENTS

(1) All documentation pertaining to application software and sensitive systems software and changes made therein shall be updated and stored securely. An up-to-date inventory 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 authorized party prior to use.

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

(4) Adequate backups of all documentation shall be maintained and a copy of all critical documentation and manuals 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 unauthorized access, loss of and damage of information outside normal working hours.

17. NETWORK COMMUNICATION SECURITY

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

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

(3) Prior authorization from the Network Administrator shall be obtained before making any changes to the network configuration.

(4) Threats and risk assessment of the network after changes in the network configuration shall be reviewed.

(5) The network shall be monitored for security irregularities which shall, when identified, be dealt with through a formal procedure.

(6) Physical access to communication and network sites shall be controlled and restricted to authorized individuals.

(7) Network diagnostic tools such as spectrum analyzer and protocol analyzer shall be used on a need basis.

18. FIREWALLS

(1) Intelligent devices generally known as “Firewalls” shall be used to isolate organisation’s data network and external networks, or to limit network connectivity between the organisation’s data network and external networks.

(2) Networks that operate at varying security levels shall be isolated from each other by appropriate firewalls.

(3) The internal network of the organisation (intranet) shall be physically and logically isolated from the Internet and any other external connection b a firewall.

(4) All firewalls shall be subjected to thorough tests for vulnerability before being put to use and at least half yearly thereafter.

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

19. CONNECTIVITY

(1) Organisations shall establish procedure for allowing connectivity of their computer network or computer system to other computer systems or networks outside the organisation.

(2) The permission to connect to other computer networks shall be approved by the network administrator and documented.

(3) All unused connections and network segments should be disconnected from the active network.

(4) Computer systems/personal computers or outside terminals accessing an organisation’s host computer system shall adhere to the general system security and access control guidelines.

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

(6) 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, security and functioning of the network.

(2) The Network Administrator shall regularly undertake the review of the network and also provide physical, logical and procedural safeguards for its security.

(3) The system security system must include a mechanism for alerting the Network administrator of possible breaches in security such as unauthorized access, virus infection and hacking.

(4) Only authorized and legal software shall be used on the network.

21. CHANGE MANAGEMENT

(1) Change Control

(a) Procedure for tracking and managing changes in application software, hardware and data in the production system shall be established.

(b) Organization's responsibilities for the change management processes shall be established.

(c) A risk and impact analysis, classification and prioritization process shall be established.

(d) Authorization procedure for change control shall be defined and documented.

(e) No changes to the production system shall be implemented until such changes have been formally authorized.

(f) Owners and users shall be notified of all changes made to the production system which may affect the processing of information the said production system.

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

(h) Version changes of application software and all system software installed on the computer systems and all communication devices shall be documented.

(i) Different versions of the application software and systems software must be kept in safe custody.

(2) Testing Changes to the production system

(a) All changes in computer source proposed in the production system shall be tested and test results shall be reviewed and accepted by all concerned bodies before implementation.

(b) All user acceptance tests in respect of changes in computer resource in production system shall be performed in a controlled environment, which includes: Test Objectives, documentation test plan, and acceptance criteria.

(3) Review of Changes

(1) Procedures shall be established for an independent review of program changes in the production environment to detect unauthorized or malicious codes.

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

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

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

(4) Problem Reporting and Management

(1) Procedures for identifying, reporting and resolving problems such as non-functioning Certification Service Provider'' system, breaches in information technology security, and hacking shall be established d communicated to all personnel concerned.

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

(5) Emergency Preparedness

(1) Emergency response procedures for all activities related to with computer operation shall be developed and documented.

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

(6) 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) A business continuity plan shall be developed which shall 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 depending on the business needs.

(7) Disaster Recovery/Management

(1) Disaster recovery plan shall be developed, properly documented, tested and maintained to ensure that in event of a failure of the information system or destruction of the computer facility, essential level 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) fallback procedure describing the actions to relocate activities or support services to a back-up site; and

(c) restoration procedures describing the actions to be taken to return to normal operations at the original site.