THE UNITED REPUBLIC OF TANZANIA

PRESIDENT'S OFFICE

PUBLIC SERVICE MANAGEMENT

# Human Capital Management Information System Security Guiding Principles

May, 2014

# TABLE OF CONTENTS

# ABBREVIATIONS

**CEO**, Chief Executive Officer

**CIRT**, Critical Incident Reporting Team

**DHCM**, Director of HUMAN Capital Management

**DICTS**, Director of Government Information, Communication and Technology Services

**DRP**, Disaster Recovery Plan

**e-GA**, e-Government Agency

**HCMIS**, Human Capital Management Information System

**ICTS**, Information and Communication Technology Services

**ISIM**, Information Security Incident Management

**ISO**, Information Security Officer

**IT**, Information Technology

**LAN**, Local Area Network

**LGAs**, Local Government Authority

**MDAs**, Ministries, Department and Agencies

**NDA**, Non-Disclosure Agreement

**PC**, Personal Computer

**PO-PSM**, President's Office Public Service Management

**PS**, Permanent Secretary

**RAS**, Regional Administrative Secretary

**USER ID**, Unique User Identifier

**VPN**, Virtual Private Network

# PREFACE

The Government has implemented the Human Capital Management Information System (HCMIS) which possesses information that is sensitive and valuable. The exposure of such information to unauthorized individuals can cause irreparable damage to the Government business operations. Additionally, if HCMIS information is tampered with or made unavailable, it can impair the Government's ability to manage the public service.

The purpose of these Security Guiding Principles for HCMIS is to define a set of security requirements that will assist in protecting the HCMIS from information security threats that could compromise confidentiality, integrity and availability of the system to all users at all times. The HCMIS Security Guiding Principles have been developed in consideration of importance of HCMIS to the Government and hence the needs to ensure that the system is secure and can be trusted by all stakeholders. These Security Guiding Principles therefore have been developed to achieve the following goals:-

- to communicate to every user their responsibilities for the protection of the HCMIS information;
- to increase awareness amongst the HCMIS users and stakeholders on the importance of information;
- to manage the security risks and associated threats to the information resources of the HCMIS; and
- to provide and protect a secure environment for the retention and dissemination of HCMIS information.

These Security Guiding Principles therefore require all employees who have been given access to the HCMIS, to diligently take measures to protect HCMIS information as appropriate to the sensitivity level. Failure to comply with these Security Guiding Principles may result into disciplinary action as per existing public service rules and regulations.

I am confident that every HCMIS user will comply with the HCMIS Security Guiding Principles, so that HCMIS is kept secure and available all the time.

George D. Yambesi

**PERMANENT SECRETARY (ESTABLISHMENTS)**

# SCOPE

These Security Guiding Principles apply to all Employers, Human Resource Officers, Personnel Action Approvers, Payroll Officers, Printer Operators, ICT Technical Personnel and Third Parties, who have access to HCMIS information or infrastructure. Compliance with these Security Guiding Principles is mandatory.

These Security Guiding Principles are specific to HCMIS. They address electronic information that is created, stored or used in support of the business activities of HCMIS, including the associated infrastructure and Human Capital.

# THE SECURITY GUIDING PRINCIPLES

## PART 1: Information Security Guiding Principles

Objective: To provide management direction and support for information these Security Guiding Principles have been issued in accordance with the business requirements and relevant laws and regulations.

Clauses:

1. The Security Guiding Principles document shall be approved by Management of the Office of Establishment, published and communicated to all employees and other relevant external parties.
2. The Security Guiding Principles shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.
3. There shall be a defined information risk assessment process that shall be executed at least once a year and whenever there is a major change in the information system environment.

## PART 2: Responsibility (Organization of Information Security)

Objective: To manage information security within the organization and to maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to or managed by external parties.

Clauses:

1. Roles and Responsibilities
   a. **Permanent Secretary (Establishment):**
      The Permanent Secretary Establishment shall:
      - Approve the HCMIS Security Guiding Principles.
      - Assign responsibility related to HCMIS system to Employers.
      - Monitor compliance and periodically review compliance reports.
      - Provide sufficient resources to facilitate implementation of the HCMIS Security Guiding Principles.

   b. **Information Security Committee:**
      The Information Security Committee will consist of key personnel within HCMIS. Members of this committee shall be Chief Executive Officer – eGovernment Agency (Chairman), Director of Government ICT Services, Director of Human Capital Management, Director of Treasury Computer Services, Assistant Director HCMIS, Assistant Director HCM and Assistant Director Payroll Management.
      The Information Security Committee will be responsible for governance and oversight of the HCMIS information security program. The Information Security Committee will have responsibility for the following items.
      - to recommend implementation of new initiatives to maintain and enhance these Security Guiding Principles
      - to analyze and manage institution risks

- to review and recommend policies, procedures and standards
- to ensure consistency in disciplinary processes for violations

c. **Critical Incident Response Team (CIRT)**

The team will ensure that there is capacity to provide help to users when a security incident occurs in the system.

The Critical Incident Response Team will consist of 6 members from IT Audit (1), IT Technical team (3), Government Security Office (1) and PO-PSM Legal section (1). The team will be selected by the Permanent Secretary, Establishment.

Depending on the magnitude of the incident, the team may require support from other Institutions that respective areas of expertise is needed.

They will be responsible for:

- Advisory
- Vulnerability and Penetration testing
- Incident response
- Malicious code analysis
- Liaison with Law enforcement
- Incidence post-mortem and reporting

d. **Information Security Officer:**

The Director of Government ICT Services will serve as Information Security Officer. The Information Security Officer will have responsibility for the following items.

- to implement and maintain these Security Guiding Principles
- to implement and maintain an information security training program
- to implement and maintain the information security architecture to support these Security Guiding Principles

- to generate HCMIS Security Guiding Principles compliance reports
- to control the security of HCMIS information assets
- to proactively monitor HCMIS information assets relative to potential security threats
- to investigate and respond to information security incidents
- to report information security incidents to the Permanent Secretary, Establishment
- to design a disaster recovery plan to ensure the continuity of HCMIS business operations in the event that information systems become unavailable for an extended period of time
- to provide information security recommendations to the Permanent Secretary, Establishment relative to mitigating the risks associated with information security threats that could negatively affect HCMIS business operations

e. **Information Owners:**

All Accounting Officers will be Information Owners for the Officers under their mandate.

Information Owners will have responsibility for the following items.

- to classify the information resources within their area of responsibility
- to determine the access rights (who should have access) and privileges (what access should be provided) for information resources within their area of responsibility
- to communicate to the Information Security Officer the legal requirements for access and disclosure for the information resources within their area of responsibility

f. **Information Technology Staff:**

Government ICT Services Directorate under President's Office – Public Service Management will serve as the Information Technology department and will have responsibility for the following items.

- to implement access rights and privileges as defined by Information Owners
- to implement Disaster Recovery Plan
- to implement backup and recovery procedures for centrally-maintained information resources
- to provide the computer infrastructure necessary to support HCMIS operations
- to provide the data network infrastructure necessary to support HCMIS operations

g. **Employer / Accounting Officer:**

The Accounting Officer (Employer) is responsible for managing HCMIS information assets.

The employer shall be responsible

- to oversee implementation of HCMIS Security Guiding Principles within their administrative responsibilities
- to identify and authorize appropriate individuals to be granted access to HCMIS
- to take appropriate disciplinary actions to individuals who have violated the HCMIS Security Guiding Principles
- to classify and de-classify information used within HCMIS which is under their jurisdiction.

h. **Authorized Users:**

These are system users who have been granted access to specific information assets in the performance of their assigned duties.They include Human Resource Officers, Personnel Action Approvers, Payroll Officers and Printer Operators.

The authorized users shall be responsible:

- to protect information resources in their custody or to which they have been granted access.
- to report any suspected information security incident to the appropriate Employer and the Information Security Officer

i. **Third Party:**
   All contractors, consultants, vendors and other persons working under agreements with the Government concerning anything on HCMIS, will have responsibility to protect information resources and report any suspected information security incident to the appropriate Accounting Officer and the Information Security Officer.

2. Management of MDAs and LGAs shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

## PART 3: Asset Management

Objective: To achieve and maintain appropriate protection of organizational assets and to ensure information receives an appropriate level of protection.

Clauses:

1. There shall be an inventory of critical information assets that will be updated yearly and whenever there is addition, modification or disposal of an asset.
2. There shall be defined and documented ownership of information assets.
3. Handling of sensitive electronic information assets shall be in accordance to its level of classification.
4. Employees shall return information assets after termination of responsibilities.
5. Equipment, information or software shall not be taken from the office without prior authorization of the Accounting Officer.

## PART 4: Human Capital Security

Objective: To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

Clauses:

1. Third party staff involved in exchange of information or providing support shall be vetted via normal Government vetting procedures.
2. Employees and third party staff shall observe acceptable use of information systems as stated in Appendix A: Section 1 of these Security Guiding Principles.
3. All users shall be made aware and acknowledge acceptance of their responsibilities on the information system.
4. Third party contract requirements shall clearly stipulate staff that will provide supports on each specific area. Such list shall be kept updated at all times.
5. PO-PSM shall provide regular security awareness and training to various user groups.
6. Third party organizations exchanging information with PO-PSM shall provide security awareness and training to their staff handling exchanged information.
7. Employers shall notify PO-PSM on users who undergo disciplinary proceedings.

## PART 5: Physical and Environmental Security

Objective: To prevent unauthorized physical access, damage and interference to the organization’s premises and information as well as to prevent loss, damage, theft or compromise of assets and interruption to the organization’s activities.

Clauses:

1. Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.
2. Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

# PART 6: Communications and Operations Management

Objectives:

- To protect the confidentiality, integrity and availability of information, software and information processing facilities.
- To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.
- To maintain the security of information and software exchanged within an organization and with any external entity.
- To detect unauthorized information processing activities.

Clauses:

1. PO-PSM shall define and implement information Non-Disclosure Agreement (NDA) and other relevant security requirements on exchange of information with third parties.
2. Operating procedures shall be documented, maintained, and made available to all users.
3. It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.
4. The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.
5. Detection, prevention, and recovery controls to protect against malicious code (Virus, worms, spyware, and scripts) and appropriate user awareness procedures shall be implemented as described in Virus Guideline.
6. Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup guidelines.
7. Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the

systems and applications using the network, including information in transit.

8. Storage Media shall be disposed off securely and safely when no longer required, using formal procedures as guided by “Government’s Acceptable Proper Usage of ICTs Guidelines”.
9. System documentation shall be protected against unauthorized access.
10. Information exchange through all types of communication facilities shall be secured.
11. Agreements shall be established for the exchange of information and software between the organization and external parties.
12. Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization’s physical boundaries.
13. Information transmitted through communication network shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
14. Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.
15. Information processing facilities usage shall be monitored and the results of the monitoring activities reviewed regularly.
16. Logging facilities and log information shall be protected against tampering and unauthorized access.
17. System administrator and system operator activities shall be logged and periodically reviewed.

## PART 7: Access Control

Objective: To prevent unauthorized user access to HCMIS that may lead to compromise or theft of information and information processing facilities.

Clauses:

1. System Privileges for Users who are suspected or confirmed to be involved in activities related to breach of Confidentiality, Integrity and Availability of data in the system, shall be revoked immediately while other disciplinary measures are underway.
2. The access rights of all employees, contractors and third party users to information and information processing facilities shall cease upon termination of their employment, contract or agreement, or adjusted upon change.
3. Security shall be applied to off-site equipment taking into account the different risks of working outside the organization’s premises.
4. Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets.
5. Access to information assets shall be controlled based on the business and security requirements.
6. There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.
7. The allocation and use of privileges shall be restricted and controlled.
8. Appropriate authentication methods shall be used to control access by remote users.
9. Groups of information services, users, and information systems shall be segregated on networks.
10. Access to network resources shall be restricted, in line with business and security requirements.

11. Access to operating systems shall be controlled by a secure log-on procedure.
12. All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.
13. Inactive sessions shall be terminated after a defined period of inactivity.

# PART 8: Information Systems Acquisition, Development and Maintenance

Objective:

- To ensure that security is an integral part of information systems development by preventing errors, loss, unauthorized modification or misuse of information in applications.
- To protect the confidentiality, authenticity or integrity of information by cryptographic means.

Clauses:

1. Changes to information processing facilities and systems shall be controlled.
2. Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.
3. Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.
4. Test data shall be selected carefully, protected and controlled.
5. The implementation of changes shall be controlled by the use of formal change control procedures.

# PART 9: Information Security Incident Management

Objective: To ensure a consistent and effective approach is applied to the management of information security incidents and to ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

Clauses:

1. Information security events shall be reported through appropriate management channels as quickly as possible.
2. All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.
3. Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.
4. Evidence related to information security incidents shall be collected, retained, and presented to conform to the rules for evidence laid down by the court of law.

## PART 10: Business Continuity Management

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Clauses:

1. Disaster recovery plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of critical business processes.
2. Disaster recovery plans shall be tested and updated regularly to ensure that they are up to date and effective.

## PART 11: Compliance

Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, of any security requirements and to ensure compliance of systems with organizational security policies and standards.

Clauses:

1. All relevant statutory, regulatory and contractual requirements and the organization's approach to meet security requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization.
2. Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.
3. Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.
4. Employers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.
5. Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.

## DOCUMENT CHANGE MANAGEMENT

The Information Security Officer will initiate or receive requests for changes to this Security Guiding Principles document.

The Information Security Officer will review and propose requested changes to the Information Security Committee. The Information Security Committee will review the proposed amendments and recommend them to the Permanent Secretary, Establishment for approval. Approved changes will formally be included in a revision to these Security Guiding Principles.

This Policy will at the minimum be reviewed annually.

# APPENDIX A: Policy Guidelines

## 1. Acceptable Use Guidelines

Purpose: To establish prudent and acceptable use of HCMIS.

Audience: The Acceptable Use guidelines apply equally to all individuals granted access privileges to HCMIS.

Guidelines:

1. Users must report any vulnerability in HCMIS, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the Accounting Officer or HCMIS technical team.
2. Users must not attempt to access any data or programs contained on HCMIS for which they do not have authorization or explicit consent.
3. Users must not share their HCMIS account(s), passwords, Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes.
4. Users must not make unauthorized copies of copyrighted software.
5. Users must not purposely engage in any activity that may: harass, threaten or abuse others; degrade the performance of HCMIS; deprive an authorized user access to a HCMIS resource; obtain extra resources beyond those allocated; circumvent HCMIS security measures.
6. Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, HCMIS users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on HCMIS.
7. HCMIS information must not be used for personal benefit.

8. Users are not allowed to access HCMIS information from outside Government premises without approval from Permanent Secretary, Establishments. Where such permission is granted user must adhere to Security Guiding Principles and any other guidelines of HCMIS.
9. Users must not allow family members, non-authorized Employees/Staff or other non-employees to access HCMIS.
10. Remote users connecting via the internet shall connect to HCMIS system through secure VPN.
11. Users must not extend or re-transmit network services in any way. This means users must not install a router, switch, hub, or wireless access point to the HCMIS network without approval of Permanent Secretary, Establishment.
12. Users are not permitted to alter HCMIS network hardware in any way.
13. Users are not allowed to access HCMIS through an internet café.

## 2. User Account Management Guidelines

Purpose: The purpose of User Account Management guidelines is to establish the rules for the creation, monitoring, control and removal of user accounts.

Audience: The User Account Management guidelines apply equally to all individuals with authorized access to HCMIS

Guidelines:

1. All accounts created must have an associated request and approval that is appropriate for HCMIS
2. All users must sign the HCMIS Security Acknowledgement and Nondisclosure Agreement before access is given to an account.
3. All accounts must be uniquely identifiable using the assigned user name.
4. All default passwords for accounts must be constructed in accordance with the HCMIS Password Guidelines.
5. All accounts must have a password expiration that complies with the HCMIS Password Guidelines.
6. Accounts of individuals on extended leave (more than 30 days) will be disabled.
7. All new user accounts that have not been accessed within 30 days of creation will be disabled.
8. System Administrators or other designated staff:
    a. are responsible for removing the accounts of individuals that change roles within HCMIS or are separated from their relationship with HCMIS
    b. must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes
    c. must have a documented process for periodically reviewing existing accounts for validity
    d. are subject to independent audit review
    e. must cooperate with authorized HCMIS management investigating security incidents.

## 3. Administrators Special Access Guidelines

Purpose

The purpose of the HCMIS Administrative/Special Access guidelines is to establish the rules for the creation, use, monitoring, control and removal of accounts with special access privilege.

Audience

The HCMIS Administrative/Special Access guidelines apply equally to all individuals that have, or may require, special access privilege to HCMIS.

Guidelines

1. All users of Administrative/Special access account must sign the HCMIS Security Acknowledgement and Nondisclosure Agreement before access is given to an account.
2. All users of Administrative/Special access accounts must have account management instructions, documentation, training, and authorization.
3. Each individual that uses Administrative/Special access accounts must refrain from abuse of privilege and must only do investigations under the direction of the Information Security Officer.
4. Each individual that uses Administrative/Special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
5. Each account used for administrative/special access must meet the HCMIS Password guidelines.
6. The password for a shared administrator/special access account must change when an individual with the password leaves.
7. In the case where a system has only one administrator there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.

8. When Special Access accounts are needed for Internal or External Audit, software development, software installation, or other defined need, they:

    a. must be authorized
    b. must be created with a specific expiration date
    c. must be removed when work is complete.

## 4. Backup Security Guidelines

Purpose: The purpose of the HCMIS Backup /Disaster Recovery Plan (DRP) guidelines is to establish the rules for the backup and storage of electronic HCMIS information.

Audience: The HCMIS Backup/DRP guidelines apply to all individuals that are responsible for the installation and support of HCMIS, individuals charged with HCMIS Security and data owners.

Guidelines:

1. The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.
2. The HCMIS backup and recovery process must be documented and periodically reviewed.
3. The third party providing offsite backup storage for HCMIS must be cleared to handle the highest level of information stored.
4. Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source system. Additionally backup media must be protected in accordance with the highest HCMIS sensitivity level of information stored.
5. A process must be implemented to verify the success of the HCMIS electronic information backup.
6. Backups must be periodically tested to ensure that they are recoverable.
7. Backup tapes must have at a minimum the following identifying criteria that can be readily identified by labels and/or a bar-coding system:
   a. System name
   b. Creation Date
   c. Sensitivity Classification [Based on applicable electronic record retention regulations.]
   d. HCMIS Contact Information

## 5. Change Management Guidelines

Purpose: The purpose of the HCMIS Change Management guidelines is to manage changes in a rational and predictable manner so that staff and customers can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of HCMIS.

Audience: The HCMIS Change Management guidelines apply to all individuals that install, operate or maintain HCMIS.

Guidelines:

1. Every change to HCMIS resource such as: operating systems, computing hardware, networks, and application is subject to the Change Management guidelines and must follow the Change Management Procedures.
2. All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) need to be reported to or coordinated by Information Security Officer.
3. A formal written change request must be submitted for all changes, both scheduled and unscheduled.
4. All scheduled change requests must be submitted in accordance with Change Management Procedures so that the Information Security Committee has time to review the request, determine and review potential failures, and make the decision to allow or delay the request.
5. Each scheduled change request must receive formal Information Security Committee approval before proceeding with the change.
6. The appointed leader of the Information Security Committee may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back out plans, the timing of the change will negatively impact a key business process such as year-end accounting, or if adequate resources cannot be

readily available. Adequate resources may be a problem on weekends, holidays, or during special events.

7. Customer notification must be completed for each scheduled or unscheduled change following the steps contained in the Change Management Procedures.
8. A Change Review must be completed for major changes as defined in Change Management Procedures, whether scheduled or unscheduled, and whether successful or not.
9. A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:
   a. Date of submission and date of change
   b. Owner and custodian contact information
   c. Nature of the change
   d. Indication of success or failure

## 6. Data Classification Guidelines

Purpose: The purpose of the HCMIS Data Classification guidelines is to provide a foundation for the development and implementation of necessary security controls to protect information according to its value and/or risk. Security standards, which define these security controls and requirements, may include: document marking/labeling, release procedures, privacy, transmission requirements, printing protection, computer display protections, storage requirements, destruction methods, physical security requirements, access controls, backup requirements, transport procedures, encryption requirements, and incident reporting procedures.

Audience: The HCMIS Data Classification guidelines apply equally to all individuals who use or handle any HCMIS information.

Guidelines:

1. Data shall be classified as follows:

   **Top Secret:** Information requiring the highest degree of protection because its unauthorized disclosure could cause exceptional, grave damage to the national security eg. records for United Republic of Tanzania's President, Vice President and Prime Minister including their spouses.

   **Secret:** Information or material requiring a substantial degree of protection because its unauthorized disclosure could cause serious damage or endanger national security e.g. records for Chief Secretary, Ministers, Judges, Permanent Secretaries, Member of Parliaments' Records, etc.

**Confidential:** Refer to information or material requiring protection because its disclosure could cause damage or administrative embarrassment or would be of advantage to unwanted people. e.g. Routine annual confidential reports, intelligence reports, some staff reports, Official Records such as Disciplinary records, Vetting document ,Letters of interdiction ,Medical Board reports ,Personal service particulars ,Medical report on appointment ,Personal record Card/form (including Social Security Number) .

**Open**: Refer to information or material requiring protection because its disclosure would be of advantage to unwanted people. e.g. Change of name, Letters of transfers/postings, Loan application, Request to change job, Salary slips / advice, On Job reporting letter, Details of acting appointments, Documents relating to training or study leave, Appointment letter(s) , Letters of promotion, etc.

2. Sensitive documents and records must be carefully handled according to its level of classification.
3. All Classified Documents/Records must have appropriate markings made by creators; such markings limit access to information covered by a specific document/record.
4. If the document is wrongly classified, user must consult document’s/record’s creator before de-classify it.

## 7. Incident Management Guidelines

Purpose: This document describes the requirements for dealing with computer security incidents. Security incidents include, but are not limited to: virus, worm, and Trojan horse detection, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of HCMIS as outlined in the HCMIS Security Guiding Principles and associated guidelines.

Audience: The HCMIS Incident Management guidelines apply equally to all individuals that use the system.

Guidelines:

1. HCMIS Critical Incident Reporting Team (CIRT) members have pre-defined roles and responsibilities which can take priority over normal duties.
2. Whenever a security incidentis suspected or confirmed, the appropriate Incident Management procedures must be followed.
3. The Information Security Officer is responsible for notifying the CIRT and initiating the appropriate incident management action including restoration as defined in the Incident Management Procedures.
4. The Information Security Officer is responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.
5. The appropriate technical resources from the CIRT are responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
6. The Information Security Officer, in consultation with Information Security Committee, will determine if a widespread HCMIS communication is required, the content

of the communication, and how best to distribute the communication.

7. The appropriate technical resources from the CIRT are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.
8. The Information Security Officer is responsible for initiating, completing, and documenting the incident investigation with assistance from the CIRT.
9. The Information Security Officer is responsible for reporting the incident to the:
    a. Permanent Secretary, Establishment
    b. Employers (where applicable)
10. The Information Security Officer is responsible for coordinating communications with outside organizations and law enforcement in consultation with Government Communication Unit and/or Human Resource Legal Services section.
11. In the case where law enforcement is not involved, the Information Security Officer will recommend disciplinary actions, if appropriate, to the Human Capital Management.
12. In the case where law enforcement is involved, the Human Resource Legal Services in consultation with Information Security Officer will act as the liaison between law enforcement and PO-PSM.

## 8. Internet Policy Guidelines

Purpose: To establish prudent and acceptable practices regarding the use of the internet while executing HCMIS operations.

Audience: The HCMIS Internet Use guidelines apply equally to all individuals granted access to HCMIS with the capacity to access the internet, the intranet, or both.

Guidelines:

1. Software for browsing the Internet is provided to authorized users for business use only.
2. All files downloaded from the Internet must be scanned for viruses using the approved IS distributed software suite and current virus detection software.
3. The use of the Internet must comply with the Acceptable Use guidelines.
4. All user activity on HCMIS assets is subject to logging and review.
5. All sensitive HCMIS information transmitted over external network must be encrypted.
6. Users are expected to observe carefully the User Acceptance Guideline.

## 9. Network Configuration Security Guidelines

Purpose: The purpose of the Network Configuration Security guidelines is to establish the rules for the maintenance, expansion and use of the network infrastructure.

Audience: The Network Configuration Guidelines applies equally to all individuals with access to HCMIS system.

Guidelines:

1. All network connected equipment must be configured to a specification approved by PO-PSM.
2. All hardware connected to the HCMIS network is subject to monitoring.
3. Changes to the configuration of active network management devices must not be made without the approval.
4. Network devices (Routers, Firewall and Switches) must be installed and configured to secure HCMIS system.

## 10. Password Guidelines

Purpose: The purpose of the Password guidelines is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the HCMIS user authentication mechanisms.

Audience: These guidelines apply equally to all individuals who use HCMIS.

Guidelines:

1. Passwords must be changed at least every 90 days.
2. Passwords must have a minimum length of 8 alphanumeric characters
3. Passwords must not be easy to guess.
4. Passwords must not be reused for a period of one year
5. Passwords must not be shared with anyone
6. Passwords must be treated as confidential information

## 11. Physical Access Guidelines

Purpose: The purpose of the Physical Access guidelines is to establish the rules for granting, control, monitoring, and removal of physical access to HCMIS processing facilities.

Audience: The guidelines apply to all individuals that are responsible for the installation and support of HCMIS, individuals charged with HCMIS security, and data owners.

Guidelines

1. Physical access to HCMIS system restricted facilities must be documented and managed.
2. All HCMIS processing facilities must be physically protected in proportion to the criticality or importance of their function.
3. Access to HCMIS processing facilities must be granted only to support personnel, and contractors, whose job responsibilities require access to that facility.
4. The process for granting card and/or key access to HCMIS processing facilities must include the approval of the person responsible for the facility.
5. Each individual that is granted access rights to an HCMIS facility must sign the appropriate access and non-disclosure agreements.
6. Requests for access must come from the applicable data/system owner.
7. Access cards and/or keys must not be shared or loaned to others.
8. Access cards and/or keys that are no longer required must be returned to the person responsible for the HCMIS facility. Cards must not be reallocated to another individual bypassing the return process.
9. Lost or stolen access cards and/or keys must be reported to the person responsible for the HCMIS facility.
10. Cards and/or keys must not have identifying information

other than a return mail address.

11. All HCMIS facilities that allow access to visitors will track visitor access with a sign in/out log.
12. A proper written explanation must be provided on the event of loss, stolen or none returned access cards and/or keys which will be supported with Police Lost Report.
13. Card access records and visitor logs for HCMIS facilities must be kept for routine review based upon the criticality of the Information Resources being protected.
14. The person responsible for the HCMIS facility must remove the card and/or key access rights of individuals that change roles or are separated from their relationship with HCMIS.

## 12. Security Monitoring Guidelines

Purpose: The purpose of the Security Monitoring Policy is to ensure that Information Resource security controls are in place, are effective, and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. This early identification can help to block the wrongdoing or vulnerability before harm can be done, or at least to minimize the potential impact. Other benefits include Audit Compliance, Service Level Monitoring, Performance Measuring, Limiting Liability, and Capacity Planning.

Audience: The Security Monitoring Guidelines apply to all individuals that are responsible for HCMIS system administration and Security.

Guidelines:

1. Automated tools will provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible a security baseline will be developed and the tools will report exceptions. These tools will be deployed to monitor:
    a. Internet traffic
    b. LAN traffic, protocols, and device inventory
    c. Operating system security parameters

2. The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:
    a. Automated intrusion detection system logs
    b. Firewall logs
    c. User account logs
    d. Network scanning logs
    e. System error logs

f. Application logs
g. Data backup and recovery logs

3. The following checks will be performed at least annually by assigned individuals:

   a. Password strength
   b. Unauthorized network devices
   c. Unauthorized personal web servers
   d. Operating System and Software Licenses

4. Any security issues discovered will be reported to the ISO for follow-up investigation.

## 13. Virus Guidelines

Purpose: The purpose of the Computer Virus Detection guidelines is to describe the requirements for dealing with computer virus, worm and Trojan horse prevention, detection and cleanup.

Audience: The Virus Detection Guidelines applies equally to all individuals that use HCMIS.

Guidelines:

1. All workstations connected to the HCMIS network must use approved virus protection software and configuration.
2. The virus protection software must not be disabled or bypassed.
3. The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.
4. The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.
5. The HCMIS file server attached to the network must utilize approved virus protection software and setup to detect and clean viruses that may infect file shares.
6. Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Help Desk.
7. In case of infection to file or PC, measures of dis-infecting it should be taken while the PC is off-line.