MINISTRY OF LABOUR, SOCIAL SECURITY AND SERVICES

ICT STRATEGY

JUNE 2014

Table of Contents

Introduction 5

Glossary of Terms 6

List of Acronyms 8

Amendment procedures and ownership 9

Policy background 9

Policy Statement 9

Policy compliance 10

Policy objectives 10

Guiding principles 11

Scope 12

ICT security is defined in terms of: 13

Password policy 14

Application Development Standards 15

Standards for electronic accounts password setting 16

Firewall policy 19

Operational procedures 20

Printing policy 21

Software development and maintenance policy 22

Procedure for software development 23

Input data validation 23

Internal processing 24

Message integrity 24

Output data validation 24

Training 24

Minimum Software applications and operating systems standard 25

Procedure for Software Testing and Training 25

Protection of systems documentation 26

Guiding principles (Software maintenance) 26

Upgrades 27

Pre-implementation 28

Procedures for implementation 28

Procedures for post-implementation 29

ICT support policy 30

Server security and space usage policy 32

Tips for conserving storage space 34

E-mail communication policy 35

E-mail account termination procedure 36

Default Protection 37

Message Recording- 37

Disclaimer 39

Anti-virus Policy 40

Backup policy 41

Restoration 44

Backup Validation /Restore Testing 44

Defining requirements 45

Confirming that the backup and recovery strategy complies with: 45

Configuration data 45

Internet usage policy 45

Hardware and software acquisition policy 49

Procedures for purchase and installation of hardware and software: 50

Budgeting 50

Approval and acquisition of computer hardware 51

Identification of hardware and software 51

References 55

Introduction

Institutional efficiency and effectiveness is grounded in the establishment of and adherence to sound Policies and procedures. Operations are directly tied to policies and procedures, which are in turn a reflection of an institution's vision and goals. The Ministry of Labour, Social Security and Services automation policy will dictate how the Ministry staff will use the available Information and Communication Technology (ICT) tools for improvement in the dispensation of duties. The policy sets clear participatory requirements and boundaries for all Ministry parties involved from a business process and/or technology perspective.

The management should ensure that this policy is formalized and made operational within the Ministry. The policy takes a holistic view of the entire Ministry environment and will guide how technology is implemented and practiced.

This Policy document acts as a central repository for all current policies that govern the Ministry's ICT processes. The set of policies and procedures defined in this Policy document will need to be continuously updated and will become more robust to accommodate the Ministry's contribution to the attainment of the Vision 2030.

Therefore, this document provides a starting point for the policies and procedures that will be required in future. The Policy document draws from the experiences of the Ministry ICT Staff and from lessons learnt from other Government departments. In addition, this Policy document draws its fundamentals from global best practices, specifically Control Objectives for Information and related Technology (COBIT) and IT Infrastructure Library (ITIL) that are expected to be consistently applied, widely communicated and regularly reviewed

Glossary of terms

Term	-	Definition
Ministry	-	Means Ministry of Labour, Social Security and Services
Policy	-	This is a formal, brief and high-level statement or plan that embraces an Organization's general beliefs, goals, objective, and acceptable procedures for a specific subject area.
Vision	-	This is a statement that defines the desired or intended future state of an Organization in terms of its fundamental objective and/or strategic direction.
Mission	-	This is a statement that defines the fundamental purpose of an organization describing why it exists and what it does to achieve its vision.
Guiding Principles	-	They represent best or prudent practice applied to a specific subject matter or situation to guide a course of action.
User	-	This means any person employed by the Ministry on a permanent, temporary, consultancy basis, or any other person approved by the officer-in-charge of ICT who has been authorized access to ICT resources.
Standards	-	Specific operational requirements established by the Ministry as the authority or model to determine a course of action within the Policy.
Change	-	A change is defined as the addition, deletion, reconfiguration or alteration to the functionality of a particular component required to deliver services. Components required to deliver the services include items of hardware, system software, applications software, the data and voice network, procedures and the relationships between those items.
Virus	-	This means any program code, programming instruction or set of instructions constructed with the specific purpose of damaging, interfering with or otherwise adversely affecting computer software, computer programs, data files or operations and includes, without limitation, all viruses, Trojans, worms, zombies and time bombs.
Unauthorized use	-	This means use of Ministry computer systems and e-mail system by anyone other than an authorized user.

Non-functional - Non-functional requirements address the aspects of an application that may requirements not directly affect the functionality of the application as seen by the users, but can have a profound effect on how that application is accepted by both the users and the people responsible for supporting that application.

Firewall Environment -A firewall environment is a collection of systems at a point on a network that together constitute a firewall implementation. A firewall environment could consist of one device or many devices such as several firewalls, intrusion detection systems and proxy servers.

Intranet - An intranet is a network internal to an organization but that runs the same protocols as the network external to the organization. Every organizational network that runs the TCP/IP protocol suite is an intranet.

Backup - The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

Archive - The saving of old or unused files onto magnetic tape or other offline Mass storage media for the purpose of releasing on-line storage room.

Commercial Off The-Shelf (COTS) packages - This is a term for software, hardware or Computer products that are ready- made and available for sale, lease, Or license to the general public.

Information Custodian - This is the person responsible for overseeing and implementing the necessary safeguards to protect the information assets, at the level Classified by the Information owner.

Information Owner - This is the person who creates or initiates the creation or storage of information; he/she is the initial owner.

List of acronyms

ICT	-	Information and Communications Technology
MLSSS ICT	-	Ministry of Labour, Social Security and Services ICT
GoK	-	Government of Kenya
E-MAIL	-	Electronic mail
COTS	-	Commercial off The Shelf Packages
TCP/IP	-	Transmission Control Protocol/Internet Protocol
PDA	-	Personal Digital Assistant
SNMP	-	Simple Network Management Protocol
UPS	-	Uninterruptible Power Supply
IDS	-	Intrusion Detection System
PC	-	Personal Computer
ISO	-	International Organization for Standardization
COBIT	-	Control Objectives for Information and related Technology
ITIL	-	Information Technology Infrastructure Library
USB	-	Universal Serial Bus
VPN	-	Virtual Private Network
SSL	-	Secure Sockets Layer
SDLC	-	Software Development Life Cycle
CMM	-	Capability Maturity Model
CPU	-	Central Processing Unit

Amendment procedures and ownership

This Policy document requires that ICT policies remain current as institution's needs evolve and technology changes. These policies must be published and communicated to employees and relevant external parties.

The following considerations should be made when making the Policy amendments:

Deliberate management actions must be put in place by the Ministry's ICT Unit to ensure ICT infrastructural planning is continuously carried out and that it covers all ICT management and operations areas. They should be planned in line with the Ministry Strategic Plan.

The Policy should be reviewed on regular basis to allow for amendment to areas requiring improvement or that have undergone change.

The policies must be updated and published as need arises. The Ministry ICT Unit should facilitate regular reviews to ensure compliance.

Policy background

The Government has recognized the importance of ICT in national development as outlined in the **Millennium Development Goal**, **Kenya Vision 2030** and the **e-government strategy** among other national policies. In order to actualize these aspirations, ICT Units have been established in Government Ministries.

The Ministry of Labour, Social Security and Services in recognition of the importance of ICT in effectiveness and efficiency in service delivery has embarked on a process of modernizing operations to harness the opportunities presented by ICT. These processes must be supported by a set of policies and procedures that will enable the ministry to execute them.

Policy Statement

The purpose of this document is to provide a set of comprehensive policy guidelines to regulate the information technology use at the Ministry. The broad objective is to ensure compliance with acceptable practices, applicable laws and regulations. The policies are designed to effect proper information technology use control.

All employees of the ministry are required to take careful note of the contents of this

document and ensure that they understand and comply with both the written word and spirit of the content. Compliance with the policies by all representatives is mandatory. Ministry employees should assist one another in compliance with this document, as well as with the identification of any contraventions so that they might be remedied. The policies in the document enable the employees to comprehend the ministry's expectations as well as everyone's own obligation.

If any employee is in doubt about the application of certain policies they should discuss the matter with the person to whom they report or a person at management level responsible for implementing these policies. As the policy will be updated over time, it is the responsibility of the ministry's ICT Unit to ensure that they have the latest copy of the document available for distribution at any one time. Significant changes to this document must be recorded in the document revision history and signed off.

Policy compliance

It is the responsibility of all employees and users to read and comply with this document. Compliance with the policies set forth in this document is essential and a requirement for continued employment at the ministry. Non-compliance with this policy and any future releases will result in disciplinary action, including and not limited to termination, civil or criminal legal action as stipulated in the Code of Regulation (COR) and any other relevant circular. The ministry reserves the right to revoke the privileges of any user at any time. All users are responsible for adhering to copyright, patent laws, and license agreements for intellectual property (such as the Ministry or a third-party's software). Violations of authorial integrity may be grounds for sanctions; examples of such violations include: plagiarism, invasion of privacy, unauthorized access, and copyright violations.

Policy objectives

The purpose of the automation policy is to define operational framework that will govern the ministry in the use of ICT for improvement in the dispensation of services. By determining and communicating the policies, users of ICT within the ministry know the boundaries of ICT usage. This knowledge will prevent accidental breaches arising from poor awareness and enforcement. This policy document provides a step-by-step guidance on how to efficiently and effectively communicate and implement both new and updated automation policies.

The policy will also serve to:

- Guide the proper ICT management within the ministry;
- Support and maintain the mission critical functions of the ministry; safeguard the

privacy of individual official information;

- Protect the integrity and reputation of the ministry;
- Prevent the misuse of the ministry 's ICT systems for malicious acts; act as a compliance to national and international laws;
- Improve transparency and efficiency of the ministry; fulfill the ICT Vision and Mission;
- Successfully implement the ICT Strategies;
- Ease ICT Operations;

ICT Vision and Mission

The automation policy will strive to support the Ministry of Labour, Social Security and Services in supporting the vision and mission statements.

Vision

To be the best in the implementation of ICT skills in the Government

Mission

To mainstream ICT's policies and plans at all ministry levels

Guiding principles

The implementation of this policy shall be guided, among other things by the right of access to information, transparency, fairness and accountability. The following shall also be taken into account as key guiding principles:

- This policy is designed to guide and mainstream the use of ICT in all areas of the ministry rather than a stand-alone technology framework;
- Top management shall take leadership mainly in facilitating the mobilization of investment required for development of infrastructure backbone as well as the implementation of this policy;
- The upgrading of existing and development of new infrastructure shall also be taken into account as complimentary services to the successful rollout of the ICT infrastructure and services in order to increase penetration across the ministry;
- Priority shall be given to the establishment of coordination mechanisms at different levels to allow for integration of ICT's in key functions of the ministry in order to ensure sustainability of ICT programmes and projects;
- A deliberate and accelerated ICT manpower development and implementation plan shall form the basis for human resource development at all levels of the ministry as stipulated in the e-Government strategy.
- The implementation of this policy shall be supported by intensive and extensive

public awareness activities at all levels of the ministry. This is expected to create demand for ICT in areas such as training.

Scope

These policies also cover the usage of all Information and Communications Technology resources of the ministry, including, but not limited to:

- All computer-related equipment, including desktop personal computers (PCs), portable PCs, terminals, workstations, wireless computing devices, telecom equipment, networks, databases, printers, servers and shared computers, and all networks and hardware to which this equipment is connected;
- All electronic communications equipment, including e-mail, PDAs, wired or wireless communications devices and services, Internet and intranet, and other online services;
- All software including purchased or licensed software applications, ministry employee or vendor/supplier written applications, computer operating systems, firewalls, and any other software residing on ministry -owned equipment;
- All intellectual property and other data stored on ministry equipment;

All of the above are included whether they are owned by or leased to the ministry or are under the ministry's possession, custody, or control; and

This policy also applies to all users, whether on the ministry's property, connected from remote sites via any networked connection, or using the ministry's equipment. In addition the use of the ministry ICT resources, even when carried out on a privately owned computer that is not managed or maintained by the ICT Unit of the ministry is governed by this policy.

Critical success factors

The following factors are crucial in enhancing effective policy management:

- Regular audit of ICT policy compliance receptive change culture
- Top management commitment and support competent ICT staff
- Appropriate awareness and training for the ministry staff involvement of third parties on ICT matters
- Effective legal and regulatory framework

Security

The sensitivity of data cannot be overstated. Leaks, loss, or theft of sensitive or confidential

information can compromise the integrity of the ministry. It is imperative that there is an appreciation of the necessity of protecting ministry information where deemed appropriate and/or required by law. Properly designed security procedures will provide this capability. The ministry needs to be very secure and take adequate measures to safeguard the data and information both in transit and during storage. Moreover, access to the ministry information and services should only be provided to authenticated and authorized individuals. Adopting ICT industry-standard security practices is paramount for the ministry.

Items covered include, but are not limited to, servers, communication systems, networks, personal computers, mobile devices, Personal Digital Assistant and all forms of data including text, video, audio, imagery, and other representations used as information or in control functions.

By providing easy, universal access to the business functionality, services have the potential to greatly increase security vulnerability. Security governance should in its most elemental form, consider these questions:

Who has access to each application, service or functional component?

Who should have access to which application, service, functional component or data? How is that access controlled, managed and enforced?

What are the expected availability, reliability, Recovery Time Objective (RTO), Mean Time Between Failures (MTBF) and Time To Repair (TTR)?

What security and accountability mechanisms exist?

Have these service implementations been audited and found to be in compliance with the relevant regulations

ICT security is defined in terms of:

Confidentiality – Restricting access to information;
Integrity – Maintaining accuracy and completeness of information; and
Availability – Making information available as and when required.

Password policy

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of their change. This policy is designed to protect the organizational resources on the network by requiring strong passwords along with protection of these passwords, and establishing a minimum time between changes to passwords.

Passwords are a method of identifying and authenticating users as they attempt to gain access to the ministry computer systems. They are the entry point to the ministry's computing resources. Protecting access to these resources is pivotal in ensuring that the ministry computer system remains secure.

Scope

This Policy applies to all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any ministry station, has access to ministry network, or stores any non-public ministry information. This policy applies to all personnel who have a computer account requiring a password on the organizational network including but not limited to a domain account and e-mail account. It includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any ministry facility.

Responsibility

The ICT officers are responsible for enforcing this policy.

Guiding principles

General

Passwords are required for all users and accounts. The login identity may not be used in any form in the password, be it reversed, scrambled or repeated. The password may not include the users'initials, name, or relatives'name in any form personal information about the user such as identity number or vehicle registration may not be used in the password

Standard words as found in English or other dictionaries shall not be used

Single characters shall not be repeated (For example. 444333) A password shall contain a minimum of eight characters.
A password shall contain alphanumeric characters including a combination of uppercase, lowercase and special characters.

A password shall not be written down. Password shall be changed regularly.
Passwords shall be unique i.e. users may not use the same password presently used, or any of those used in the previously.

Passwords shall not be shared between users.

Passwords shall be kept strictly confidential and shall not be disclosed to any other staff.

All system-level passwords must be changed at least on a monthly basis.

User accounts that have system-level privileges granted through group memberships should have a unique password from all other accounts held by that user.

Passwords must not be inserted into email messages or other forms of electronic communication.

Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively.

All user-level and system-level passwords must conform to the guidelines described below.

Application development standards

Application developers must ensure their programs contain the following security precautions.

Applications should:

Support authentication of individual users, not groups.

Not store passwords in clear text or in any easily reversible form.

Provide for some sort of role management, such that one user can take over the functions of another (i.e. receive delegated roles) without having to know the other's password.

Use of passwords for remote access users

Access to the Ministry networks via remote access is to be controlled using a one-time password authentication

Standards for electronic accounts password setting

The guidelines below are generic and each system in the ministry may have its own set of password rules which ought to be adhered to.

All system-level passwords must be changed at most on a quarterly basis. All user-level passwords must be changed at least every month.

Each successive password must be unique. Re-use of the same password within 4 generations old will not be allowed.

Passwords must have a minimum length of eight (8) characters.

Names or words from the dictionary should not be used as passwords. Two or more unrelated words may be combined as a password.

A Password must contain a mixture of upper and lower case characters, numbers and punctuation marks. A strong password contains the following:

- ✓ Two or more upper case letters from the alphabet (A – Z); o Two or more lower case letters from the alphabet (a – z); o Two or more digits (0 – 9); and
- ✓ One special character (~! @ $ % ^ & * , ? /).

Passwords should not contain an individual's ID number, social security number, and date of birth, telephone number or any other information that could easily be guessed by another individual.

Passwords must not be inserted into email messages or other forms of electronic communication.

Passwords should never be written down or stored online.

Ministry staff should not use the same password for ministry accounts as for other non-ministry access (For example: personal email, online trading).

Passwords should not be disclosed to any other person whomsoever. If someone demands your password, refer him/her to this document or advice him/her to contact the ICT Unit.

Ministry staff is advised not to use the remember password feature of applications (For

example. web based applications, Microsoft outlook, outlook express e.t.c.)

Ministry staff should change or request for the change of their passwords whenever they suspects that their password has been compromised.

In addition to the above guidelines, the ICT Unit's officer's or their delegates should ensure the following:
All vendor-supplied default passwords (or other alternative access mechanisms) must be changed before any computer or communications system is used for any ministry activity;

Users must be able to change their own passwords; Passwords must be encrypted by the system; Users who will be absent from the place of business for a period exceeding 30 days must have their login suspended for the period of their absence;

Concurrent user-ID logins must be limited to one;

Intruder detection and lockout must always be activated and monitored by the ICT Unit; Incorrect login attempts must be limited to a maximum of three. After three incorrect login attempts, the password must be suspended and the ICT Unit must be contacted to reset the password (regardless of the amount of time between attempted logins);

Persons who demand to have access to passwords shall be referred to this document or have them call someone in the ICT Unit;

Users should not write passwords down and store them anywhere in the office or out of the office;

The ICT Unit may attempt to crack or guess users' passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user will be required to change his or her password immediately.

Users should not store passwords in a file on ANY computer system (including PDAs or similar devices) without encryption; and

Password cracking or guessing may be performed on a periodic or random basis by ICT Unit or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Guidelines for database passwords

In order to access any of ministry databases, a program must authenticate to the database by presenting acceptable credentials. The database privileges that the credentials are meant to restrict can be compromised when the credentials are improperly stored.

In order to maintain the security of ministry internal databases, access by software programs must be granted only after authentication of credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be word readable. Database credentials may reside on the database server. In this case, a hash number identifying the credentials may be stored in the executing body of the program's code. Database credentials may be stored as part of an authentication server.

Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials. Database credentials may not reside in the documents tree of a web server. Database authentication must not allow access to the database based solely upon a remote user's authentication on the remote host. Passwords or pass phrases used to access a database must adhere to the policy on passwords.

If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.

The scope into which you may store database credentials must be physically separated from the other areas of your code, For example, the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (For instance, the user name and password) and any functions, routines, or methods that will be used to access the credentials.

For languages that execute from source code, the credentials' source file must not reside in the same browser or executable file directory tree in which the executing body of code resides.

Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed. Database passwords used by programs are system-level passwords as defined by the Policy on

Passwords.

Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the Policy on passwords. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.
Firewall policy

Definition

It is a part of computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device(s) that is configured to permit or deny network transmission based upon a set of rules and other criteria.

Purpose

The purpose of this policy is to define standards for provisioning security devices owned and/or operated by the ministry. The intention of this policy is to outline the minimum security policy for the ministry firewall environment. These standards are designed to minimize the potential exposure of the ministry's sensitive and/or confidential data, intellectual property, damage to public image that may arise from unauthorized use of ministry's resources.

Scope

This policy applies to the ministry's workforce and essential rules regarding the management and maintenance of firewalls within an entity. Firewalls prevent unauthorized users from accessing private networks. The approach adopted to define firewall rule sets is that all services will be denied by the firewall unless expressly permitted in this policy.

The firewall will (at minimum) perform the following security services:

Access control between the trusted internal network and untrusted external networks. Block unwanted traffic as determined by the firewall rule set.
Conceal vulnerable internal systems from the Internet.
Conceal information, such as system names, network topologies, and internal user IDs, from the Internet.
Log traffic to and from the internal network. Provide robust authentication.
Provide Virtual Private Network (VPN) connectivity.

Responsibility

The ICT Unit is responsible for ensuring the implementation of the requirements of the firewall policy.

Guiding principles

A desktop firewall is needed, this is the tool used to enforce restrictions on network access by limiting port and protocol access. The firewall should limit the user's ability to change its configuration, yet provide functions such that the user can identify issues that may be caused by the firewall policy. The firewall should support port and application based filtering.

Knowledge of existing port requirements or a baseline requirements that would be as the standard or default operating system configuration used in the ministry.

Ability to deploy a single global firewall solution to all personal computers, this means deploying the solution to all personal computers in the ministry with a consistent or single policy.

Facility to provide and update the firewall policy; some firewalls can be centrally managed directly. Depending on the needs or structure of the ministry, the minimum requirements would require a common/global firewall policy that can be updated, for example through the replacement of a configuration file. Some form of central software management would need to be in place.

Traffic with invalid source or destination addresses should always be blocked Tools to aid in the analysis of the networking are required.

A training session about Internet security will act as a cohesive link with the Internet usage policy and will result in users abiding by the policy once they comprehend.

Operational procedures

The ministry employees may request changes to the firewall's configuration in order to allow previously disallowed traffic. All requests will be assessed to determine whether they fall within the parameters of acceptable risk. Approval is not guaranteed as associated risks may be deemed too high. If this is the case, an explanation will be provided to the original requester and alternative solutions will be explored.

The ministry employees may request access to the Internet for services located on the internal ministry network. Typically, this remote access is handled via a secure encrypted Virtual Private Network connection.

Firewall logs will be backed up, archived and reviewed frequently.

Printing policy

Definition

Printing is a process of re-producing text and image with ink on paper using a printing device.

Purpose

Printing represent one of the highest expenditures at ministry. The goal of this policy is to facilitate the appropriate and responsible use of ministry's printer assets, as well as control ministry's printer cost of ownership by preventing the waste of paper, toner and ink among others.

Scope

This printing policy applies to all employees of ministry, as well as any contracted employees who may be using ministry's networks and equipment.

Responsibility

Members of staff together with ICT Unit are responsible for enforcing this policy.

General principles

The relevant departments will provide printing paper and monitor usage printing must be done on back-to-back basis

Small desktop printers shall not be used to print a document of more than 30 pages. All large documents must be printed from the heavy duty network printers

Non- ministry work shall not be printed using the ministry's printing facilities.

Printers must not be used as duplicating machines. If there is need for multiple copies, print one copy and photocopy.

In order to minimize costs and improve accountability, network printers must be installed in strategic locations.

Access to the network printer must be based on domain user settings.

All printer malfunctions must be immediately reported to ICT helpdesk.

Avoid printing unnecessary documents and e-mail messages, this is wasteful. Instead, use the folders and archiving functionality in your e-mail application to organize and view your messages.

Software development and maintenance policy

Purpose

The purpose of this policy is:
To establish guidelines for software development at the ministry. This policy will allow the ministry to standardize the software development to maximize resource utilization, consistent outcome and a higher quality software product delivered to end users.

To ensure that adequate testing and training is carried out for newly developed or acquired software systems in accordance with documented requirements, standards and procedures.

To ensure existence and protection of ministry's systems documentation. This includes detailed information about a system's design specifications, its internal workings and functionalities including schematics, architectures, data structures, procedures and authorization processes.

To prevent compromise of operational Information and Communications Technology from unauthorized software maintenance and/or upgrades while reduce the risk of Information and Communications Technology functionality loss.

Scope

All software source code developed, maintained and upgraded using ministry's resources are the property of the ministry. This also includes all software developed, maintained and upgraded using personal resources that was commissioned by the ministry.

This policy covers software development for the following types of applications:

Internal management software.

Windows-based productivity suite, add-ons for Microsoft Office and others. Stand-alone and Server Operating Systems

Responsibility

The ICT Unit is responsible for enforcing this policy.

Guiding principles (Software Development)

Software developed for or by the ministry must always follow a formalized development

process which is managed under the project in question. The integrity of the ministry's operational software code must be safeguarded using a combination of technical access controls and restricted privilege allocation and robust methods.

Procedure for software development

All proposed system developments must be institutionally driven and supported by an agreed Business Case. Ownership for such enhancements will solely rest with the system owner and the ministry.

The development of tailored software is only to be considered, if warranted by a strong Business Case and supported by management and adequate resources over the expected life time of the resultant project.

Management must ensure that proper separation of duties applies to all areas dealing with systems development, systems operations or systems administration.

Disposal of software only takes place when it is formally agreed that the software is obsolete and its associated data files which may be archived will not require restoration in future.

Vendor developed software must meet the User Requirement Specification and offer appropriate product support

Testing the software to verify that it functions as intended.

Enforcing change control processes to identify and document modifications which may compromise the security controls

Using common ministry processes and services (For example, authentication, access control, financial management)

Management must ensure that the change management and communication processes are enforced.

Input data validation

Ensure the validity and integrity of data input to the new software by:

Limiting fields to accept specific ranges of data (For example, defining out of range values or upper and lower data volume limits);

Checking for invalid characters in data fields; Making key fields mandatory;

Verifying the plausibility of input data using institutional rules;

Protecting against common attacks (For example, buffer overflows); and Using control balances to verify complete input and processing.

Internal processing

Verify that the new software include audit trails to:

Detect unauthorized or incorrect changes to information; Prevent information from being accidentally overwritten;
Prevent internal information from being disclosed via software responses; Protect against common attacks (For example, buffer overflows);
Check the integrity, authenticity or any other security feature of data or software downloaded or uploaded between central or remote computers;

Provide error and exception reports.

Message integrity

Determine message integrity requirements during the definition phase of system development or acquisition to prevent errors, loss, unauthorized modification or misuse of information in Information and Communications Technology.

Output data validation

Verify that processes are documented to validate the data output from the software by:

Reconciling control balances to verify that data is processed accurately; Verifying the plausibility of output data using institutional rules;
Providing sufficient information for a reader or subsequent software to determine the accuracy, completeness, precision and classification of the information;

Maintaining audit trails; and providing error and exception reports.

Training

Document the training requirements and communicate them as part of the Terms of Reference for the systems implementation.

Ensure that education and training includes:

Proper use and protection of information;
The Ministry's process based training;
All functional aspects of the system;
The system security features;
The systems technical training include backups, restorations, and programming environment management; and
All operational requirements of the system

Minimum software applications and operating systems standard

When software is designed to run on a system that has a keyboard, product functions shall be executable from the keyboard.

Applications shall not disrupt or disable activated features of other products that are identified as accessibility features, where those features are developed and documented according to the industry standards.

Applications also shall not disrupt or disable activated features of any operating system that are identified as accessibility features where they have been documented by the manufacturer of the operating system

Procedure for software testing and training

The use of live data for testing new system or system changes may only be permitted where adequate controls for the integrity and security of the data are in place.

New systems must be tested for capacity, peak loading and stress. They must demonstrate a level of performance and resilience which meets or exceeds the technical and institutional needs and requirements.

Normal system testing methods will incorporate a period of parallel running prior to the new or amended system being acceptable for use in the live environment.

Training is to be provided to ministry staff involved in the functionality and operations of new systems.

New and enhanced systems must be fully supported at all times by comprehensive and up-to-date documentation. New systems or upgraded systems should not be introduced to the live environment unless supporting documentation is available.

Protection of systems documentation

Information custodians and owners must ensure that documented procedures for the secure use and storage of system documentation are established and adhered to.

Procedures must:
Require information classification labeling of system documentation;

Establish lists of users authorized to access system documentation on a need to know' basis;

Establish handling rules for the information regardless of storage media (For example., electronic, paper);

Require use of access controls, passwords, encryption or digital signatures as appropriate to the information classification; and

Include a compliance process.

Guiding principles (Software maintenance)

Maintenance of commercial-off-the-shelf software

Other than vendor supplied patches, Commercial-Off-The-Shelf (COTS) software must not be modified unless necessary. This requirement must be documented and approved by information owners and custodians.

If changes to COTS software are required, information owners and custodians must determine:

The impact the change will have on the security controls in the software; o If consent of the vendor is required;

If the required functionality is included in a new version of the software; and

If Ministry will become responsible for maintenance of the software as a result of the change.

If changes are made to COTS software the original software must be kept unaltered and must be:

Logged and documented, including a detailed technical description; o Applied to a copy of the original software; and

Tested and reviewed to ensure that the modified software continues to operate as intended.

Applying vendor supplied patches and updates

A software update management process must be maintained for COTS software to ensure:

The most up-to-date approved patches have been applied; and o The version of software is vendor supported.

Upgrades

Information owners and custodians must implement procedures to control software installation on operational software to ensure that:

Updates are planned, approved, impacts assessed, tested, logged and have a rollback plan;

Personnel and end users must be notified of the changes, potential impacts and if necessary undergo additional training;

New releases of software are reviewed to determine if they will introduce new security vulnerabilities;

Modifications to operational software are logged;

The number of personnel able to perform the updates is restricted

Development code or compilers are not present on operational software; o Vendor supplied software is maintained at the supported level.

Any software upgrades must be properly tested by the ICT Unit and users before they are used in any live environment.

The decision to upgrade any software is only to be taken after consideration of the associated risks of the upgrade and weighing these against the anticipated benefits and necessity for such change.

All Ministry application software is provided with the appropriate level of technical support to ensure that Ministry's critical processes are not compromised by ensuring that any software

problems are handled efficiently

Operating system(s) of any of the Ministry's computer systems and office suites should be upgraded to the latest version of the software.

Pre-implementation

Before an updated or new software is implemented into the operational environment, checks should be performed to ensure that:

A Security Threat and Risk Assessment has been carried out;

A Privacy Impact Assessment has been performed and approved;

Performance and capacity requirements can be met and supported by the Ministry

Development problems have been resolved successfully; o The effects on existing operational software are known;

Arrangements for fall-back have been established if the updated or new software fails to function as intended.
Before the updated or new software is implemented into the operational environment: o Communicate changes to users who may be affected by the change;

Error recovery and restart procedures should be established; o Business continuity plans should be developed or updated; o Operating procedures should be tested;

Users should be educated to use the software correctly and securely; and

Computer operators/system administrators should be trained on how to run the software correctly and securely.

Procedures for implementation

The installation process should include:

o Validating the load or conversion of data files; o Installing executable code and not source code; o Source code to be handed over to the Ministry o Providing ongoing technical support;

o Implementing new or revised procedures/documentation; o Discontinuing old software,

procedures and documentation; o Arranging for fall-back in the event of failure;

- Informing the individuals involved of their roles and responsibilities;
- Transferring responsibility of the software from development teams to operational teams to ensure separation of duties; and
- Recording installation activity.

Procedures for post-implementation

Post-implementation reviews should include:

The efficiency, effectiveness and cost of security control;

Lessons learned and scope for improvements of security controls; and o Security incidents and mitigation

ICT support policy

Definition

"ICT support" is defined as any queries made by end users to the ICT unit regarding any failures, problems, issues, questions, and other matters relating to the operation and continuity of Ministry owned personal computers, servers, web sites, software, peripherals, telephony, mobile devices, and other equipment or assets.

Purpose

The purpose of this Policy is to describe the basic level of service that will be guaranteed by the ICT Unit. It also identifies and delineates the limits of ICT's capabilities.

Scope

The range of support offered and guaranteed by the ICT unit will vary depending on the nature of the problem, the number of staff or resources available to resolve the problem, the criticality of the asset in question, and other factors regarding the nature of the support requested. Priority will be given to mission-critical applications/workflows/assets first, moving down in priority sequence.

Contact

The ICT support team can be contacted through;

ICT Unit, 1st floor, room 112 NSSF building, Eastern wing block A 2727980/4 Ext 2115,2138,2135,2113

Email: info@labour.go.ke

Policy

The following policy statements exclude the support of employees' personal computing equipment, peripherals, software, and services, unless prior telework or mobile working arrangements have been made according to ministry policies.

1. **Software Support:** Support is provided for all core software packages and operating systems on ministry workstations, servers, laptops, and other computing equipment. Support is also provided for department-specific software applications. Specifically, support is provided for:
MIS-OVC-CT, IFMIS, IPPD, IRMS, Ms Office, Operating Systems Systems and Databases

Please note that personally installed or unlicensed software, including screensavers, games,

applications whose publishers are no longer in business, etc., will not be supported by the ICT unit. Unauthorized installation of certain software is illegal and in violation of the ministry policies.

2. **Hardware support:** Support is provided for all core hardware and devices, including PC motherboards, peripherals, network interface cards, hard drives, storage devices, and so on. All cases of suspected hardware faults will be diagnosed accordingly. The ICT unit will fix hardware defects but may need to send equipment back to the vendor/manufacturer when need be. Wherever possible, replacements will be made for the end user in such cases. Specifically, support is provided for: Computers, Scanners, Printers, UPS, Photocopiers among others

Please note:
That personally installed or unapproved hardware, including speakers, unauthorized monitors, personal cell phones, etc., will not be supported by the ICT unit. Unauthorized installation of certain hardware is illegal and in violation of ministry's policies.

Unauthorized personnel should not be allowed to offer support to ministry ICT equipment.

3. **Remote support:** All remote access will be centrally managed by ministry's ICT unit and will utilize encryption and strong authentication measures. Remote access connections covered by this Policy include (but are not limited to) Internet, dial-up modems, Frame Relay, ISDN, DSL, VPN, SSH, cable modems, proprietary remote access/control software, etc.

4. **Determining support:** Telephone support will be the mode of choice for most minor problems and difficulties. The ICT unit will conduct on-site support at the end user's workstation where applicable. Remote support will be provided for teleworkers or mobile workers who are within a reasonable driving distance from the office. Otherwise, telephone support will be provided, unless the user is able to bring the equipment in for inspection. Walk-in support is not encouraged for users who show up at the ICT unit unless absolutely necessary. Exceptions might be made in emergency situations, but these will be assessed on a case-by-case basis.

5. **Enforcing support:** The ICT unit reserves the right to monitor hardware and software installation and usage on Ministry's computer systems. The Unit will conduct periodic audits to ensure compliance with this ICT support policy. Adhoc audits may be conducted, during such audits, scanning for and removal of rogue hardware may also be performed. Unauthorized software may also be uninstalled at this time.

6. **Personal support:** As mentioned earlier in this policy, support will not be granted for personally owned software and hardware. In cases where a business case can be made for an

employee using personal equipment for ministry purposes (e.g. via a teleworking or telecommuting arrangement), then support may be granted. This policy, refrains end users from approaching ICT staff for assistance for personal hardware and/or software.

Server security and space usage policy

Purpose

The purpose of this policy is to;

Establish standards for the base configuration of ministry internal server equipment.

Effective implementation of this policy will minimize unauthorized access to information.

To preserve the finite amount of storage space available on network servers. This policy is designed to curtail the increasing use of company server space for unauthorized, non-business-related files.

Scope

This policy applies to server equipment owned and/or operated by ministry and to servers registered under any Ministry's internal network domain.

Responsibility

ICT personnel working on behalf of the ministry are responsible for enforcing this policy.

Guiding Principles

Ownership and Responsibilities:

All internal servers deployed at the ministry must be owned by the ICT Unit that is responsible for system administration. Approved server configuration guides must be established and maintained by the ICT Unit. The Unit should monitor configuration compliance and implement a policy tailored to their environment. The Unit must establish a process for changing the configuration and space usage guides, which includes review and approval by management.

Servers must be registered within the ministry's system.

The following information is required to positively identify the point of contact:

- ✓ Server contact(s) and location, and a backup contact, Hardware and Operating System/Version,
- ✓ Main functions and applications, if applicable, and
- ✓ Information in the ministry system must be kept up-to-date.
- ✓ Configuration changes and usages for production servers must follow the appropriate

change management procedures.

Configurations

Operating System configuration should be in accordance with approved technical guidelines. Services and applications that will not be used must be disabled. Access to services should be logged and/or protected through access-control methods such as Transfer Control Protocol (TCP) Wrappers.

The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with the ministry's requirements.

Trust relationships between systems are a security risk and should be avoided. Do not use a trust relationship when some other method of communication will do.

Always use standard security principles of least required access to perform a function.

Do not use root when a non-privileged account will do. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels

Servers should be physically located in an access-controlled environment. Servers are prohibited from operating in uncontrolled cubicle areas.
Monitoring all security related events on critical or sensitive systems must be logged and audit trails saved as follows:

All security related logs will be kept online for a minimum of a week.
Daily incremental tape backups will be retained for at least a month.
Weekly full tape backups of logs will be retained for at least a month.
Monthly full backups will be retained for a minimum of 2 years.
Archives should be kept offsite in Government institutions o Evidence of unauthorized access to privileged accounts

Security-related events will be reported to management, who will review logs and report incidents to the ICT Unit. Corrective measures will be prescribed as needed. Security related events include, but are not limited to port-scan attacks.

Compliance

Audits will be performed on a regular basis by authorized ICT staff in the Ministry.

Audits will be managed by the internal audit group or management, in accordance with the

Audit policy. Management will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for appropriate action. Every effort will be made to prevent audits from causing operational failures or disruptions.

Appropriate files for storage

Files that directly pertain to the business of the ministry may be saved on the server. These include official files created through the use of ICT Unit approved and installed software.

Inappropriate files include unofficial related Media Player3s (MP3), Graphical Interchange Format (GIF), games, executables and any other employee installed software not approved by the ICT Unit. These files consume valuable server space and can introduce damaging viruses into the network.

Attempts will be made to block the storage of all un-official files. If such files are detected on the server the user will be asked to delete them immediately.

Storage space allocation

Each employee will be allotted a minimum of 100MB for their PC's home directory.
However, requests for more server storage space can be granted by the ICT Unit if need be.

Alerts will be sent to all employees who are close to exceeding their server space quota. If an employee exceeds their server space quota, they will be unable to save files until sufficient allocated space. If an employee needs support in freeing storage space he or she may contact the ICT Unit.

Tips for conserving storage space

It is the responsibility of every employee to ensure that they use their server storage space allocation properly. Each employee should set aside time on a monthly basis to ensure that they remain within their space quota.

Identify, remove and/or archive items that are:

Outdated, such as preliminary draft versions of current documents; Out-of-use or orphaned files;
Duplicated files; and Un-official or non-critical files.

E-mail communication policy

Purpose

The purpose of this policy is to ensure that all ministry personnel (excluding the casual workers) should have official electronic mail accounts for correspondence. The policy also describes the standards that users are expected to observe when using these email facilities and ensures that users are aware of the legal consequences attached to abuse of the facilities. The policy establishes a framework within which users of these email facilities can apply self regulation to their use. It is designed to advise users of this facility that the use will be monitored and in some cases recorded. It also states that the ministry management will investigate both internal and external complaints on abuse of this facility.

Scope

This policy applies to all permanent employees of the ministry.

Responsibility

The ICT Unit is responsible for the creation of shared correspondence e-mail account.

Guiding principles

Confidentiality-

Confidential material shall not be sent, transmitted or otherwise disseminated by users to third parties unless:

The user is duly authorized to send, transmit or disseminate confidential material

It is in the ministry's best interest to send, transmit and disseminate since it is in the public domain

The intended recipient is entitled to receive such data or material

All existing and newly confirmed permanent employees must be issued with a ministry mail account to facilitate communication between the employee, ministry and/or other employees of ministry.

Employees whose services have been detached from the ministry must have their accounts de-activated immediately upon notification from the Human Resource Management

Employees shall have only one (1) e-mail account within the ministry

Personal data concerning any user or any third party that may be kept as part of ministry records shall not be disclosed to anyone without the prior authorization of the user or third party concerned and of the relevant Head of Department.

New e-mail account creation procedure

In the event of a required shared correspondence email account, the concerned department sends its request for creation of a desired account using a standard designed form

In an event of a new employee, the Human Resources Management shall request for the creation of a new employee e-mail account

Upon receipt of a duly filled user account form, the ICT Unit checks it for completeness and must ensure the following details have been filled out:
First and last name, Title, Department/section, Workstation

The ICT Unit then creates an e-mail account in accordance with the Ministry's e-mail standard.
The e-mail account created is communicated to the user with a "Welcome e-mail" and the user manual detailing the Policy.

E-mail account termination procedure

In an event of an officer's detachment, the Human Resource Management will forward the list of the officers to ICT Unit to deactivate the e-mail account.

E-mails may be forwarded to the new forwarding addresses for 14 days after deactivation upon receipt of approval.

Ministry e-mail standard

The employee user ID must consist of the employee first and middle name initials followed by a surname before inclusion of the @ labour.go.ke phrase. For example, (first name middle name initial surname@ labour.go.ke) Mar Wam Muthir email account will be mwmuthir@labour.go.ke

Sharing and forwarding

Electronic mail accounts are for specific individuals and must not be shared.

If an electronic mail message contains sensitive information, users must not forward it to another recipient unless:

The originator approves the forwarding and it is encrypted in accordance with the policy on Encryption and Digital Signatures;

The other recipient is authorized to view the information; or

The forwarding of e-mail messages without a legitimate purpose under circumstances likely to lead to embarrassment of the original sender or in violation of the clearly expressed intention or request of the original sender to restrict further dissemination is prohibited

The use of the blind carbon copy feature in electronic mail systems is discouraged because it is inconsistent with the open and honest communication at the ministry.

Broadcast electronic mail message facilities should not be employed unless head of Department/section approval is first obtained, but the use of selected distribution lists is both advisable and permissible without such approval.

Default protection

Electronic mail is not protected from prying eyes by default. Accordingly, users must be careful about the inclusion of sensitive information in electronic mail messages that are not protected by encryption. To protect information from unauthorized disclosure, users must employ encryption facilities approved by the ICT Unit.

Message recording

By default all electronic mail messages are recorded in logs and back-ups. This means that even though an electronic mail message may have been deleted from a user's in-box, it may still be retrievable with other methods. Nonetheless, because electronic mail messages which are 12 months old will be purged from the systems and users are responsible for saving important messages which might be needed at a future date.

Retention of E-Mail- Due to storage limitations and ensuring fast system responses as recommended by the vendor‘s administration guidelines, E-mail stored in user mailboxes on the e-mail servers older than 30 days will be removed from the system by the users. It is up to the users to ensure that any important e-mail is moved to either their network file storage areas or personal computer storage areas. Each user has limited disk space for the storage of e-mails. It is the responsibility of the user to ensure sufficient space is available by carrying out regular housekeeping duties on their e-mail folders. In practice, this means:

Always delete unwanted e-mail.

Large attachments should be saved to the local disk and then deleted from the mail store.

E-mails that are required to be retained for longer should be archived to a personal folder, remembering this is also limited disk space and should therefore be cleaned out on a regular basis.

Unwanted and Unsolicited E-mail (SPAM) when received, should be deleted where possible without opening.

Contents of Messages- Users must not use profanity, obscenities, or derogatory remarks in any electronic mail messages discussing employees, customers, competitors, or others involved with the Ministry. Such remarks, even when made in jest, may create legal problems such as trade libel and defamation of character. Special caution is warranted because back-up and archival copies of electronic mail made by third parties may actually be more permanent and more readily accessible than traditional paper communications.

The Ministry's Information and Communications Technology must not be used for the exercise of a user's right to free speech. Sexual, ethnic, and racial harassment including unwanted telephone calls, electronic mail, and internal mail is strictly prohibited and is cause for disciplinary action. Users are encouraged to respond directly to the originator of offensive electronic mail messages, telephone calls, and/or other communications. If the originator does not promptly stop sending offensive messages, staff must report the communications to their supervisor and the Human Resources Management Section.

No Excessive Use- Users may not make excessive use of Ministry's e-mail system to send or receive messages of a personal nature subject to the following limitations:

A level of use that is reasonable and not detrimental to the main purpose for which the facilities are provided

Priority must be given to use of resources for the main purpose for which they are provided

Personal use must not be of a commercial or profit-making nature or for any other form of personal financial gain

Personal use must not be connected with any use or application that conflicts with an employee's obligations to the ministry

Personal use must not be connected to any purpose or application that conflicts with the

ministry's rules, regulations, policies and procedures

Personal use must comply with all relevant policies and regulations.

General restrictions- The ministry's e-mail system may not be used to initiate, send, forward or receive:

Any chain-message or other message which asks the recipient to forward such message to multiple other users unless required for work and informational purposes;

Unsolicited commercial e-mail to persons with whom the sender does not have a prior relationship;

Frequent and/or numerous e-mail messages with the intention of disrupting or inconveniencing the receiver;

Any attachment of any prohibited material

Restrictions on certain personal use- Ministry e-mail system may not be used for the personal dissemination or storage of personal advertisements, solicitations, promotions, destructive programs, political material, or any prohibited material.

Users should not disguise their identity while using ministry e-mail system. Users should not alter indication of the origin of an email message.
Users shall ensure that every e-mail message which is transmitted for and on behalf of ministry shall contain the disclaimer below at the end of every such message. The disclaimer message shall be copied verbatim onto every e-mail message.

Disclaimer

Note:
This email message and any file(s) transmitted with it is intended solely for the individual or entity to whom it is addressed and may contain confidential and/or legally privileged information which confidentiality and/or privilege is not lost or waived by reason of mistaken transmission. If you have received this message by error you are not authorized to view, disseminate, distribute or copy the message without the written consent of the Ministry of Labour, Social Security and Services (MLSSS) and are requested to contact the sender by telephone or e-mail and destroy the original. Although MLSSS takes all reasonable precautions to ensure that this message and any file transmitted with it is virus free, MLSSS accepts no liability for any damage that may be caused by any virus transmitted by this email.

In order to indicate the privacy of any particular e-mail message, the user shall designate any such message as private and store it in a folder identified as private. The location and description of such folder shall be furnished to the ICT Unit and nothing in this clause shall derogate from any legitimate right of the ministry to monitor or access such messages.

Any formal document of the ministry which any user wishes to transmit via email, shall be sent as an attachment. The attachment shall be on ministry's letterhead template provided for this purpose.

Users are reminded that all e-mail attachments are compressed using ministry's standard compression software. The onus is on the user to ascertain whether the recipient received the e-mail complete with attachments.

All formal e-mail messages are ministry records. The ministry reserves the right in its discretion to access and disclose all legitimate messages sent over the ministry's e-mail system.

Anti-virus policy

Definition

An antivirus is protective software designed to defend computer against malicious software which includes viruses, Trojans, key-loggers, hijacker, dialers and other code that vandalizes or steals computer contents.

Purpose

This Policy serves to ensure that the ministry's data and the infrastructure supporting its applications are protected from malicious code. It establishes requirements which must be met by all computers in the Ministry to ensure effective virus detection and prevention.

Scope

This Policy applies to all ministry's computers that are stand-alone or on the network. This includes, but not limited to desktop computers, laptops as well as file, mail and proxy servers.

Responsibility

Ministry employees are responsible for implementation and the ICT Unit shall enforce the policy.

Guiding principles

Email attachment:

All email attachments should be scanned at the firewall level prior to reaching the user level. Virus scans should be done automatically by the system. Without exception, Antivirus

software, firewalls strategies should be deployed across all Personal Computer (PCs) with regular virus definition updates and scanning across servers, PCs and laptops.

Software:

Software is only to be installed by ICT Unit and any other authorized persons. Disks and programs from external sources are not to be used in the ministry. Upon installation of virus detection and prevention software, users must ensure:-

That the latest ministry approved anti-virus protection software has been permanently enabled;

That any data received by a user via disk, flash disk, Internet, e-mail or any other source, a comprehensive scan of that data is performed prior to loading it onto ministry computer system;

That they are trained on how to scan the viruses

That upon detection of a virus which cannot be deleted, notify ICT Unit immediately;

That only the ministry approved virus protection software is installed and it is the latest version

Limited Access:

A user's access may be limited to certain directories and write access may be limited to those directories where executable files are stored.

Backup policy

Definition

A backup is a copy of a program or file that is stored separately from original.

Purpose

The purpose of this policy is to provide for the continuity, restoration and recovery of critical data and systems. This is meant to protect data in the ministry to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data or disasters.

The purpose of the systems backup is to provide a means to:

Restore the integrity of the computer systems in the event of a hardware/software failure or physical disaster, and

Provide a measure of protection against human error or the inadvertent deletion of important files.

The systems backups will consist of regular, full and incremental backups. They are not intended to serve as an archival copy or to meet records retention requirements.

Scope

The policy applies to the ministry's units, departments and third parties who use computing devices connected to an ministry's network or who process and/or store critical data owned by the ministry.

Responsibility

Ministry employees are responsible for implementation this policy.

Guiding principles

In order to ensure that all essential services and facilities are restored as quickly as possible following an ICT system failure, back-up copies of stored data will be taken at regular intervals as determined by the Head of ICT, dependent upon the criticality and quantity of the data concerned. It is advisable to automate the backup operations.

Instructions for re-installing data or files from backup should be fully documented and should be regularly tested to ensure that they enable the systems/relevant file to be re-loaded in cases of system failure.

Restoration procedures shall be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.

Uninterruptible Power Supply (UPS) will be installed in the data centre that can support the systems during a blackout for duration to be agreed and documented in the detailed procedures by ministry.

All ministry servers will be designed with significant hardware redundancy and fail over capabilities. All critical servers will have full-time support from vendors with a guaranteed response time to be agreed upon by ministry.

For data consistency and availability, the server rooms should be connected to alternative uninterruptable power supply.

If a catastrophic event occurs to the facilities, such as fire and earthquake and there is irreparable damage caused to the systems, the environment would have to be rebuilt on new

computer equipment. The downtime in this case will be agreed upon by the ministry and documented in the detailed procedures. The procedures will also document in detail the implementation of disaster recovery measures, such as preparing a hot site or standby system at another location.

A minimum level of back-up information, together with accurate and complete records of the back-up copies and documented restoration procedures, shall be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site. At least three generations or cycles of back-up information shall be retained for critical applications.

Back-up information shall be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site. The controls applied to media at the main site shall be extended to cover the back-up site.

The retention period for essential ministry information and any requirement for archive copies to be permanently retained shall be determined collectively by the ministry.

Information owners and custodians must define and document backup and recovery processes. This should entail:

Types of information to be backed up,
Schedules for the backup
Backup media management (For example, retention period, pattern of backup cycles),
Methods for performing, validating and labeling backups, and o Methods for validating recovery of the information

Information Custodians must conduct a Security Threat and Risk Assessment to identify safeguards for backup facilities and media that are commensurate with the value and sensitivity of the information and Information and Communications Technology.

Some of the safeguards are:

Use of encryption to protect the backed up information;
Use of digital signatures to protect the integrity of the information;
Physical and environmental security;
Access controls;
Storage of media adhering to manufacturer recommendations for storage conditions and maximum shelf-life; and
Remote storage of backup media at a sufficient distance to escape any damage from a disaster at the main site.

Procedures

Backup frequency-. Exceptions to the standard procedure are permitted when justified. All exceptions must be fully documented. The standard procedure for systems' backup is as follows:

Media Rotation-Incremental backups will be performed daily on the servers and their success is controlled from the reports. The backups will be retained for one month, at which time the backup media will be recycled or destroyed.

Backup media must be replaced at the first sign of deterioration and be labeled to show age, and date due for replacement, according to the manufacturer's recommendations.

Archives are made at the end of every financial year. User account data associated with the file and mail servers are archived one month after they have left the ministry.

Restoration

Users that need files restored must submit a request to the ICT Unit through the officer in charge of ICT. Inclusion of information about the file creation date, the name of the file, the last time it was changed and the date and time it was deleted or destroyed.

All backup media that is not re-usable shall be thoroughly destroyed in an approved manner. Backup media that is used for other purposes shall be thoroughly erased.

System data will be backed up, labeled and packed securely. The date each media was put into service shall be recorded on the media. Backup media that have been used longer than twelve months shall be discarded and replaced as found appropriate.

Backup Validation /Restore Testing

Periodic tests of the backups will be performed to determine if files can be restored. Both partial and full restore tests are done. A full Policy on the restoration process should be configured and attached as part of the Backup Policy. Accountability has to be ensured in the testing process.

General

In order to ensure that our essential services and facilities are restored as quickly as possible following an ICT system failure, back-up copies of stored data will be taken at regular intervals as determined by the officer in charge of ICT, dependent upon the importance and quantity of the data concerned.

Where programs and data are held in Ministry's systems or other multi-user system, such security is likely to be covered by existing procedures. In the case of other ICT systems

(including PCs) the user will normally need to make security copies of their data. Security copies should be clearly marked as to what they are and when they were taken and stored away from the system to which they relate in a restricted access fireproof location and/or off site.

Instructions for re-installing data or files from backup should be fully documented and security copies should be regularly tested to ensure that they enable the systems/relevant file to be re-loaded in cases of system failure.

Defining requirements

Information owners and custodians must define and document backup and recovery processes that reflect the security classification and availability requirements of Information and Communications Technology including:

Confirming that the backup and recovery strategy complies with:

Official continuity plans, and
Policy, legislative, regulatory and other legal obligations.
Documenting the backup and recovery processes including:
Types of information to be backed up, Schedules for the backup of information

Backup media management (For example, retention period, pattern of backup cycles),

Methods for performing, validating and labeling backups, and o Methods for validating recovery of the information

Configuration data

Regular backups for configuration data (including their change logs) for the following facilities must be maintained and protected from unauthorized access:

Network devices Servers

Computer hardware Peripheral hardware

Internet usage policy

Purpose

Internet usage policy provides employees with rules and guidelines about appropriate use of

ministry equipment, network and Internet access. It educates Internet users about web-borne threats and how irresponsible browsing can result in malicious packages being unknowingly downloaded onto a computer which in turn could infect the whole network. It dictates what is deemed to be appropriate Internet browsing behaviour in the workplace. It also outlines appropriate and inappropriate use of ministry's Internet resources, including the World Wide Web, electronic mail, the intranet, FTP (File Transfer Protocol), and USENET. This Policy typically enforces time restrictions for employees when browsing the Internet for non work-related tasks as well as stipulating what genres of sites they are allowed to browse.

Scope

This policy applies to all employees who are connected to the ministry's network. It is not intended to deny them access rights to the Internet whilst at work but to help the users understand why visiting certain sites or downloading software onto their workstations could be detrimental to the ministry's network.

Responsibility

The ICT unit will be responsible for enforcing this Policy.

Guiding principles

The Internet Policy can be enhanced through the following ways:
It is the ministry's policy to restrict Internet use to appropriate purposes, the performance of work related duties and professional training and education.

Conservation of Network and Systems Resources. Internet traffic affects ministry network computer infrastructure by using network bandwidth, storage and computer resources. Conserve these resources and protect system response time.

Unless specifically authorized otherwise, users may not transact on behalf of ministry via the Internet (i.e. purchase of goods or services) Users are strictly prohibited from posting sensitive information such as usernames, passwords, security codes or Server-specific information which could assist third parties wishing to gain unauthorized access to ministry computer system;

Users are prohibited from publishing or transmitting confidential information on or via the Internet. If a situation exists where prohibited information has to be transmitted, written approval will be required from the management prior to the transmission or publication of such information on or via the Internet

Excessive Internet usage without valid work reason is prohibited;

Ministry may apply the use of filters in respect of certain websites, which it deems to be undesirable (whether or not such websites contain prohibited material or not).

All information taken off the Internet should be considered suspect until accompanied by validated information from another source. There is no quality control process on the Internet, and a considerable amount of information on the Internet is outdated, inaccurate, and in some cases deliberately misleading. Similarly, it is relatively easy to spoof (makes a message appear as if it came from an authorized user/ address) the identity of another user on the Internet. As a result, users must not rely on the alleged identity of a correspondent via the Internet unless the identity of this person is accompanied through methods approved by the management (digital certificates, digital signatures, etc.).

Users must not post ministry's information in public discussion groups, chat rooms, or other public forums on the Internet unless they have been preauthorized by the appropriate level of management to make this type of representation on behalf of ministry.

Users may download data files from the Internet, but must check these files for viruses before executing them (decompression and decryption, when they are used, must be performed first).

Secure Sockets Layer (SSL) which is an on-line session is acceptable. Users must not include sensitive parameters in electronic mail messages sent through the Internet unless these messages are encrypted with software approved by the ICT Unit. Users must not send any sensitive parameters such as credit card numbers, telephone calling card numbers, fixed passwords, or customer account numbers through the Internet unless the connection is encrypted

Users must not misrepresent, obscure, suppress or replace their own or another user's identity on the Internet or on any other Ministry Information and Communications Technology. In all instances, the user name, electronic mail address, Ministry affiliation, and related contact information must reflect the actual originator of a message or posting. The use of anonymous re-mailers or other identity hiding mechanisms is forbidden as explained in the e-mail and communication Policy. The use of web browsers, anonymous FTP log-ins, and other methods established with the expectation that users do not need to identify themselves is permissible.

Ministry computers or networks may only be connected to third party computers or networks once the ICT Unit has determined that the combined systems will be in compliance with ministry security requirements. Similarly, real-time connections between two or more in-house ministry computer systems must not be established unless the ICT Unit has first determined that such connections will not jeopardize information security. Connections of internal ministry computers to ministry internal network (intranet) do not require such permissions; unless the involved systems store Confidential or Highly Restricted Information. Likewise, connections to the Internet through ministry firewalls do not require such

permissions.

Staff must not connect their own computers to ministry computers or networks without prior authorization from the ICT Unit. Likewise, personally owned systems may not be used to process any ministry information unless the systems have first been approved for use by the ICT Unit.

Staff and vendors working for ministry must not make arrangements for, or actually complete the installation of voice or data lines with any carrier, unless they have first obtained written approval from the Officer in-charge of the ICT unit.

All connections between ministry internal networks and the Internet (or any other publicly-accessible computer network) must include an approved firewall or related access control system. The privileges that will be permitted via this firewall or related access control system will be based on ministry needs, and will be defined in an access control standard issued by the ICT Unit.

Although the Internet represents a valuable information resource for legitimate business and technical research and information sharing, it also presents a significant opportunity for abuse, lost employee productivity and potential liability for both ministry and the employee. The following are examples of activities, which could result in revocation of Internet access privileges or other disciplinary action that are in force:-

Personal activities that incur additional costs to ministry or interfere with employee‘s work performance.

Unlawful activities, including sending or receiving copyrighted materials, in violation of copyright laws or license agreements.

Sending or retrieving sexually explicit or offensive messages, cartoons or jokes, ethnic slurs, racial epithets or any other statement or image that that might be construed as harassment, disparagement or libel.

Sending the ministry‘s proprietary or confidential materials to anyone not entitled to know or possess them.

Users should not use the ministry ‘s Internet access to conduct any other business other than for official reasons, provided that in certain circumstances the ministry may permit limited use of such access for personal matters if such usage would enhance the productivity of the user;

Users should not use ministry Internet access to host or display personal web pages; Users

may not download any documents or images not related to ministry 's business or that have been specifically excluded;

Users should not post images or data which constitutes prohibited material;

Users are not permitted to harass or disrupt any other person whilst connected to the Internet;

Users should not knowingly introduce viruses into the ministry's computer system;

Users are prohibited from accessing websites, which contain prohibited material.

Hardware and software acquisition policy

Purpose

The purpose of this policy is to provide guidelines for the acquisition, installation of ICT equipment, software, and peripherals that are acquired for the ministry which connect to the ministry's network and/or require support of ministry's technology resources. It defines the methods of software acquisition within the ministry which will ultimately control costs by acquiring the correct type of license and optimize software and hardware value by potentially reusing or redistributing. It also ensures that installation of hardware and software is done in a quality and cost effective approach for the ministry to achieve optimal benefits.

Scope

This policy applies to all computer equipment and peripherals which connect to the ministry network. These include, but not limited to PC, laptops, software, file servers, printers, copiers, and Blackberries. It also applies to all computer software that consists of detailed programmed instructions that control and coordinate the computer hardware components in an information system and other software.

Responsibility

ICT Unit is responsible for enforcing this policy

Guiding Principles

Designated individuals from each department/Unit will submit request for technical advice and specifications of ICT equipment to the officer in charge of ICT and will be responded immediately.

A request to purchase specialized items shall be reviewed by the ICT Unit to ensure compatibility with existing standards and equipment and/or support requirements. The ICT

Unit shall complete its review within 14 days of receipt of the request. If, after review, the ICT Unit cannot approve the proposed purchase, it may ask the requesting department to reconsider its request or suggest an alternative.

Technical Evaluation will be done promptly by an appointed committee or the ICT Unit upon receipt of the quotations/tender documents.

If the proposed purchase is not approved by the ICT Unit, and a proposed alternative is not accepted, the requesting department/section may appeal the decision to the Management at the next scheduled meeting. Further appeals must be made to the Authorizing Officer.

The ICT Unit shall establish and update annually, a list of standard hardware, peripherals and software for purchase.

The installation of all above mentioned items will be installed by the ICT Unit as and when required.

Software shall not be duplicated or distributed for use except as allowed by the individual software system purchase and/or usage agreements. The ICT Unit shall maintain an inventory of all the ministry software and hardware and shall keep a database of software licenses in order for the software to be registered, supported, and upgraded as needed. Software/hardware must be registered in the name of the ministry.

Procedures for purchase and installation of hardware and software:

All hardware and software must be purchased through a structured procurement and evaluation process.

All new hardware and software installations are to be planned formally and notified to all concerned parties ahead of the proposed installation date.

New installation requirements which have an effect to the policy shall be circulated to all concerned parties, well in advance of installation.

Budgeting

The purchase of computer hardware such as PCs, printers, memory, hard disks and associated software - new or replacement, will only be purchased in accordance with the overall ministry procurement plan. Respective departments/sections should identify ICT needs before the end of each financial year and discuss these requirements with the ICT Unit.

When purchasing computer hardware and network points, such purchases will be charged to the individual department's budget or another appropriate project budget set aside for tracking hardware purchases.

When purchasing new hardware or program upgrades, such purchases will be charged to respective departmental budgets. The purchase will be done through the procurement Unit with the assistance of ICT Unit for technical quality assurance. When making the justification for purchasing ministry equipment, computer hardware, software, network connections and training costs must be considered at the same time.

Approval and acquisition of computer hardware

To purchase hardware, users must obtain the approval of their Head of Department. All acquisitions must comply with the prevailing Financial Regulations and related procedures and policies of the ministry.

Hardware and software acquisition channels are restricted to ensure that:

Ministry secures value for money on its purchases

The ICT Unit of the ministry has a complete inventory of all hardware purchased and shall label, support and upgrade such items in accordance with the license arrangements

The equipment fits within ministry procurement plan and will work with existing ministry network and operating systems.

Identification of hardware and software

The ICT Officer has overall responsibility for the completion of the identification details Hardware and software must be identified with the name of the office and department in which they will be used. Due to personnel turnover, hardware should not be identified with the name of the individual user.

The ICT Unit shall manage an inventory of all ministry hardware assets and maintain a library of all software licenses.

The software library will contain:

Title and publisher of the software;

Date and source of software acquisition;

Location of each installation as well as the serial number of the hardware on which each copy of the software is installed; Name of the authorized user; Existence and location of back-up copies and software product's serial number.

The hardware inventory will contain:

- asset number;
- serial number;
- name of supplier;
- date supplied;
- machine specification;
- Department and location of hardware;
- Purchase price; and
- Employee responsible.

Ministry's computers are valuable assets and must be both licensed and virus free. Only software purchased through the procedures outlined above may be used on ministry's computer.

Ministry owned software cannot be taken home and loaded on a user's home computer even if it also resides on his/her ministry computer.

The operational requirements of new systems shall be established, documented, and tested prior to their acceptance and use. For each system, patches will be tested by the person designated by officer in-charge of the ICT Unit.

The software must comply with Software Development Life Cycle (SDLC) Software evaluation Puts into consideration the following factors;
Quality- is it error free in its program code?

Efficiency- in terms of CPU time, memory capacity or disk space

Flexibility- can it handle -institutional requirements without much modification? o Security- does it provide control procedures for errors and improper use?
Connectivity- is it web-enabled?

Documentation- is the software well documented? Does it include help screens and helpful software agents?

Hardware- is it compatible with the existing hardware?

Cost – does it meet the budgeted costs in terms of initial and maintenance costs?

System Acceptance- Requirements and criteria for acceptance of new systems should be clearly defined, agreed, documented and tested. New data systems, upgrades and new versions shall only be migrated into production after obtaining formal acceptance.

Prior to formal acceptance being provided the following shall be ascertained:

Performance and computer capacity requirements are met,

Error recovery, restart procedures and contingency plans have been addressed, Preparation and testing of routine operating procedures are defined,
Agreed set of security controls are in place, Effective user manual is developed,

Business continuity arrangements are in place,

Installation of the new system will not adversely affect existing systems, particularly at peak processing times,

The effect the new system has on the overall security of the Ministry

Training in the operation or use of new systems has been performed, and Ease of use, as this affects user performance and avoids human error.

Implementation
The installation process should include:

- ✓ Validating the load or conversion of data files; o Installing executable code and not source code; o Providing ongoing technical support;
- ✓ Implementing new or revised procedures/documentation; o Discontinuing old software, procedures and documentation; o Arranging for fall-back in the event of failure;
- ✓ Informing the individuals involved of their roles and responsibilities;
- ✓ Transferring responsibility of the software from development teams to operational teams to ensure separation of duties; and

- ✓ Recording installation activity.

Procedure for software acquisition:
Determine that the new software acquisition is ministry's driven and is supported by an

agreed Business Case. Ownership for such enhancements will solely rest with the system owner.

Management must ensure that proper separation of duties applies to all areas dealing with systems acquisitions.

Vendor developed software must meet the User Requirement Specification and offer the appropriate product support.

Testing the software to verify that it functions as intended;

Enforcing change control processes to identify and document modifications or changes which may compromise security controls or introduce security weaknesses;

Use of standard ministry processes and services (For example, authentication, access control, financial management).

References

1) The Constitution of the Republic of Kenya
2) Ministry of Labour, Social Security and Services Strategic Plan
3) E-government Strategy, 2004
4) Kenya Vision 2030
5) Data Protection Act 1998
6) Computer Misuse Act 1990
7) Information and Communications Act 2009
8) Code of Regulations (COR)-revised 2006
9) Circulars