



HOME AFRIKA LIMITED

ICT POLICY

SEPTEMBER 2018

Version 2.0

TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	3
ACKNOWLEDGEMENT	4
DOCUMENT OVERVIEW	5
Purpose of the ICT Policy.....	5
List of abbreviations	6
INTRODUCTION	7
The Guiding principles for HAL ICT policies.	7
1.0 RISK MANAGEMENT	9
1.1 Risk Analysis	9
1.2 Risk Management.....	9
1.3 Monitoring and Evaluation	10
2.0 INFORMATION COMMUNICATION TECHNOLOGY POLICIES	11
Introduction	11
2.1 Firewall Policy.....	11
2.2 Remote Access	12
2.3 Encryption Policy	12
2.4 Wireless Policy	13
2.5 Password Policy	13
2.6 User Account Administration	14
General User Identification and Security Guidelines	14
Transferred or Terminated Users.....	15
2.7 Antivirus Policy	16
2.8 IT Configuration and Patch Management Policy	17
Overview.....	17
Principles	17
Requirements.....	17
Execute the plan	17
Patch Management.....	17
2.9 Internet and E-mail Policy	18
Acceptable use	18
Unacceptable Use	18
Website Advertising	19
2.10 Audit Trails.....	20
Denial of Service	21
Cyber security Measures	21
2.11 Incidence Handling and Response.....	21
2.12 ICT Equipment Handling	22
Damage, Loss, and Theft.....	22
3.0 PRIVACY AND DATA PROTECTION	23
3.1 Data Privacy Laws.....	24

4.0 PHYSICAL AND ENVIRONMENTAL CONTROLS.....	25
5.0 CHANGE MANAGEMENT POLICIES.....	26
4.1 Obligations.....	26
4.2. Change Control Responsibilities	26
4.3. Change Control Environment	27
4.4. Documentation	27
5.0 ASSET MANAGEMENT	29
5.1 Copyrights and License Agreements	29
5.2. Acquisition Guidelines	29
5.3. Disposal Guidelines.....	31
6.0 BUSINESS CONTINUITY MANAGEMENT POLICIES.....	32
6.1. Backup Policy	32
6.2. Media Storage	32
6.3. Restoration of Data.....	32
6.5. Disaster Recovery	33
7.0 Incident Management.....	35
7.1 Reporting of Security Violations	35
7.2 Network Security Monitoring	36
7.3 Use of Intrusion Detection Systems	38
7.4 Compliance Monitoring.....	38
8.0 IT HUMAN RESOURCES	39
9.0 CONCLUSION	40
10.0 MONITORING AND EVALUATION.....	41
11.0 APPROVAL.....	42
12.0 APPENDIX	43
12.1 Appendix I.....	43
12.2 Appendix II.....	44
12.3 Appendix III.....	45
12.4 Appendix IV	46
12.5 Appendix V	47

EXECUTIVE SUMMARY

The use of Information Communication Technology (ICT) is very vital in enabling HAL towards achieving its vision of becoming a world class real estate developing company to meet the massive demand for housing in Kenya.

The purpose of this ICT Policy is to establish a context for implementing security and control over the use of computerized information systems and equipment at HAL. Dependency on information technology to provide effective operation of the business and service delivery in modern world is a necessity. It is essential, therefore, that the ICT infrastructure and Systems be secure from destruction, corruption, unauthorized access and breach of confidentiality whether accidental or deliberate. All forms of information need to be protected, regardless of the medium (e.g. hardcopy documents, removable & local hard drives, cloud storage or during transmission over networks) used for communication or storage. All HAL's employees and contractors are responsible for protecting the organization's information. To accomplish this, the ICT policy will establish proper safeguards to protect information from accidental or intentional unauthorized modification, destruction, and disclosure. It establishes standards and guidelines to protect HAL's information assets stored in its distributed computing platforms and provide a framework for the continued development of these rules as the processing environment changes.

ACKNOWLEDGEMENT

The HAL's ICT policy development has been through team work. Sincere gratitude goes to all those who have participated in the formulation of Home Africa Limited (HAL) Information Communications Technology Policy. Special gratitude goes to Board of Directors, Senior Management and the ICT team. In addition to the internal team, we acknowledge Career Management Centre for providing guidance during the development of this policy.

DOCUMENT OVERVIEW

Purpose of the ICT Policy

This policy aims to define a framework for the development and implementation of ICT policies, strategies and services; and define the role of the Company's Information Technology Unit.

List of abbreviations

Abbreviations	Description
HAL	Home Afrika Limited
BCM	Business Continuity Management
BCP	Business Continuity Plan
BOD	Board of Directors
ICT	Information Communication Technology
KM	Knowledge Management
ERP	Enterprise Resource Planning
MTP	Medium Term Plan
IPsec	Internet Protocol Security
SAN	Storage Area Network
SLA	Service Level Agreement
SSH	Security Shell
TCP	Transmission Control Protocol
SWOT	Strengths, Weaknesses, Opportunities and Threats
IA	Internal Audit

INTRODUCTION

HAL has developed an ICT policy that will be used to guide the information communication technology investments within the organization as it seeks to align itself to real estate development initiatives. It is expected that this will be achieved by working in partnership with national, continental and global organizations championing research and development for sustainable built environment. For this to happen, the company needs to strengthen its information technology capacity to support its vision and mission. This will be achieved through the consistent implementation of the standard and guidelines outlined in this policy document.

This policy establishes institutional guidelines that will integrate the use of ICT into HAL operations for effective service delivery as outlined in the Home Afrika Strategy 2.0. It will address the need to transform HAL into a more effective and efficient company through information, knowledge sharing and process automation.

The Guiding principles for HAL ICT policies.

This policy has been derived from a set of standard IT standards as described below:

ISO 17799-2005 - establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management.

Control Objectives for Information and Related Technologies (COBIT) - an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT emphasizes regulatory compliance, helps organizations to increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework.

Information Technology Infrastructure Library (ITIL) - a widely adopted guidance for IT service management worldwide. It is non-proprietary best practice that can be adapted for use in all business and organizational environments.

IT Governance Institute (ITGI) standards - The IT Governance Institute (ITGI) was established in recognition of the increasing criticality of information technology to enterprise success. ITGI

conducts research on global practices and perceptions of governance of IT for the business community. ITGI aims to help enterprise leaders understand how effective governance can make IT successful in supporting the enterprise's mission and goals.

These standards consist of the following ten Information Technology Components;

- IT Risk Management
- Information Security
- Privacy
- Data Protection
- IT Physical and Environmental Management
- Change Management
- Asset Management
- Business Continuity Management
- Incident Management

1.0 RISK MANAGEMENT

Overview

Risk analysis involves examining the probabilities and the possible consequences of undesirable events that would negatively impact HAL Information. It identifies threats to be managed in the context of risk management. Risk management aims to reduce, but not necessarily eliminate, the frequency of a threat and its impact if it occurs. Risks can be accepted, transferred, or mitigated.

1.1 Risk Analysis

In general, risk analysis is comprised of four major activities:

- Identification of potential negative impacts or those risks that could compromise HAL's activities ‘
- Threat assessment - the determination of the likelihood of a threat
- Vulnerability assessment - the determination of the degree of seriousness of a weakness that could be exploited;
- Risk assessment - which is the result of the combination of asset valuation with the levels of potential threats and vulnerabilities to form measures of risk. Threats can be accidental, such as software malfunction or natural disaster, or deliberate, such as disgruntled persons and computer hackers.

1.2 Risk Management

Risk management identifies the countermeasures to be implemented in order to reduce risk to an acceptable level. One of the purposes of these practices is to identify a common set of countermeasures to protect HAL Information.

In order to effectively protect the information, environment and data that belongs to HAL; the concept of “need-to-know” must be implemented. Need-to-know supports authorized access and sharing of HAL Information within and across business functions for those who can demonstrate a legitimate business need and obtain access approval from the HAL unit responsible for the HAL Information.

Requirements

- I. Risk analysis should involve some quantitative or qualitative methodology to determine threats, vulnerabilities, impacts, and measures of risk.
- II. Risk management for HAL Information requires a set of common, cost-effective controls including:

- Utilization of individual access security controls within applications, systems, and infrastructure of HAL's computing and communication resources;
- Limits on access to all HAL Information based on need-to-know;
- Assurance through audit trails of system and application access, edit, and delete activity; and
- Provisions for on-going employee and user awareness.

1.3 Monitoring and Evaluation

Internal Audit (IA) will be charged with the responsibility of reviewing the risk management practices within the IT function. The IA function shall:

- Review the process of risk identification within IT and assess the adequacy of the process and risk register developed from the process
- Review the adequacy of controls designed to mitigate against the risk and test the operating effectiveness of those controls over a defined period of time.

2.0 INFORMATION COMMUNICATION TECHNOLOGY POLICIES

Introduction

Computer information systems and networks are an integral part of operations at HAL thus the organization has made a substantial investment in human and financial resources to source and implement these systems. These policies and directives have been established in order to:

- Implement identified IT strategies
- Protect ICT investment
- Safeguard the information contained within these systems
- Protect the reputation of HAL

2.1 Firewall Policy

All external and wireless connections to HAL networks must pass through a network firewall. Each network firewall must have a rule set specific to its purpose and location on the network. Network firewall configuration rules and permissible services rules must not be changed unless there is a justifiable reason. Any change to an external connection or to the configuration of the firewall must be adequately tested and documented.

All HAL network firewalls must be physically located in ICT data centres and accessible only to those whose roles and responsibilities permit them to access network firewalls. These secure spaces must also have adequate physical security measures installed.

An audit of network firewalls will be done bi-annually. These audits must also include the regular execution of vulnerability scanning on server security

Services and applications on the server that will not be used must be disabled. Access to enabled services shall be logged and/or protected through access-control methods such as TCP wrappers.

Trust relationships between systems are a security risk, and should not be used for any servers. Always use standard security principles of least required access to perform a function. Root shall not be used when non-privileged account can suffice.

Servers shall be physically located in an access-controlled environment and privileged access shall be performed over secure channels, (e.g., encrypted network connections using SSH or IPsec).

The ICT Manager will facilitate the process of keeping the software up to date with the latest software releases from the vendors (if operationally feasible), so that patches that fix security bugs are installed in a timely manner. The most recent security patches must be installed on the server as soon as practical, the only exception being when immediate application would interfere with applications running on the server.

System Administrators should be very cautious about root password or Administrator password. The password should not be stored as plain text or written down on paper. Encryption utilities should be used if the password has to be stored in a file for some reason. A back up of the file should be stored on paper or other media in a physically secure place such as a safe which is accessible to someone of integrity, but who does not do routine system administration.

2.2 Remote Access

It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to HAL internal networks through their accounts. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.

All computers connected to HAL internal networks via VPN or any other technology must use the most up-to-date anti-virus software and by using VPN technology with personal equipment, users must understand that their machines are an extension of HAL's network, and as such are subject to the same rules and regulations that apply to HAL owned equipment.

Mobile computing and storage devices containing or accessing the information resources at HAL must be approved prior to connecting to the company's information systems. This pertains to all devices connecting to the network regardless of ownership (Bring Your Own Device –BYOD). Mobile computing and storage devices include, but are not limited to: laptop computers, iPads, Tablets, Mobile Phones, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), memory cards, modems, handheld wireless devices, wireless networking cards, and any other existing or future mobile computing or storage device that may connect to or access the information systems at HAL.

2.3 Encryption Policy

Devices and Media Requiring Encryption: Encryption is required for all laptops, workstations, and portable drives that may be used to store or access sensitive data. The IT department will provide, install, configure, and support encryption software on all company laptops, PCs and mobile devices.

Electronic Data Transfers: Any transfer of sensitive data shall take place via an encrypted channel. If the encryption method includes a password, that password must be transferred through an alternative method, such as calling the individual. Email messages containing encrypted data may never include the password in the same message as the encrypted data.

Physical Transfer of Electronic Data: Any time sensitive is placed on a medium such as a CD, DVD, or portable drive to facilitate a physical transfer that data must be encrypted. Archiving sensitive data to a physical medium is not recommended, but is permitted if the

data is encrypted. All archiving shall be done electronically, so that it is stored in a controlled data center and backed up by the ICT department

2.4 Wireless Policy

All wireless infrastructure devices that reside at any HAL site and connect to HAL's network, or provide access to information classified as confidential or sensitive shall:

- Be installed, supported, and maintained by the approved IT support team.
- Use approved authentication protocols and infrastructure.
- Use approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked
- Not interfere with wireless access deployments maintained by other organizations.
- Wireless access is for HAL employees only. All other parties requiring wireless access will be required to use guest Wi-Fi network with the approval of the IT manager.
- HAL staffs are not permitted to share Wi-Fi access credentials with external parties.
- Only company devices will be allowed to connect to office Wi-Fi.
- Wi-Fi login credentials will be under the custody of ICT staff only and they are responsible for connecting all devices to Wi-Fi.

2.5 Password Policy

All user-level passwords (e.g., application user, email, web, desktop computer, etc.) shall be changed every 30 days and are required to be complex, at least 8 characters long. Passwords shall be changed immediately if they become, or are suspected of having become compromised.

A password shall not be the same as any of the previous ten passwords used for the same account.

Passwords shall require a combination of at least three of the following characteristics: alpha, numeric, upper and lower case, or special characters.

Initial passwords for all new user accounts, or reset passwords assigned when the user has forgotten the password, shall be given to users in a secure manner. The use of third parties or unprotected (clear text) electronic messages shall not be used. Initial or reset passwords shall only be valid for the first log-on and thereafter users shall be required to change the password.

System and Security Administrator passwords (e.g., root, Administrator, System) shall be a minimum of twelve characters long. System and security administrative passwords shall be changed immediately whenever there is a change in administrative responsibility.

Passwords shall not be identifiable with the user (such as first name, last name, spouse name friends, relations, colleagues, or other easily guessed names).

The User ID shall be locked and users prevented access to the network after a maximum of 3 consecutive invalid login attempts for that User ID.

Passwords shall not be shared or communicated via any electronic means that may be intercepted and compromised by unauthorized persons.

The User IDs for users with privileges such as root, administrator or supervisor shall never be suspended as their suspension could create a denial of an essential service. In lieu of suspension for such accounts, there shall be a time delay that increases with each invalid attempt, so as to make brute force guessing attacks infeasible.

Default vendor passwords shall be immediately altered following installation of systems or software.

2.6 User Account Administration

All HAL Employees shall notify their supervisors when there is any change in their user account (i.e., access to an additional system required, system access no longer required, higher/lower level in access is required).

Human Resource Management shall:

- Inform IT department in advance about new recruits, staff transfers, redeployment or termination of employment contracts.
- Hand over the HR Policy, HR Staff Code of Ethics and Conduct Manual to new staff which will include detailed security policies and Consent to be Bound form.

Departmental Heads/Managers shall:

- Notify IT department whenever they become aware of a change in the status of one of its users.
- Approve all changes in user accounts.
- Continually evaluate user privileges on the basis of need to know and least privilege.

Information Owners shall:

- Approve and monitor the access of users to data for which they are responsible.

User Administration Personnel shall:

- Administer user accounts in accordance with this policy and standards.

General User Identification and Security Guidelines

In addition to the general Application and System Security Minimum Baseline Standards, the following policies will be affected:

Approval of User ID Issuance: The information owner will approve user IDs based on a documented need and job function.

Notification of User Job/Function Changes: Supervisors and Managers must notify the IT department of changes in the employee's job function in order to ensure that access privileges are appropriately adjusted.

Notification of Extended User Absences: Supervisors and Managers will formally notify the IT department of extended absences (e.g., long-term sick leave, temporary transfers, etc.) in order to ensure that computer access is temporarily revoked.

User ID Expiration Dates for Non-Employees: For contract employees and consultants, an ID expiration date that coincides with the conclusion of the contracted project will be created.

Privileged Accounts: Users granted privileged access (i.e. access to system security mechanisms, etc.) will use a different account name than that of normal user.

Auditing User Accounts: On a quarterly basis, information security and system administrators will conduct an audit of current user accounts to ensure that the accounts of unauthorized users have been removed.

Application Access Restrictions: Access to HAL application resources will be restricted to authorized users. All access to application system resources will be protected by assigning individual user rights.

Authorization Based on Need: Authorization to modify data or execute commands, transactions or programs, or other access to production data will be defined on a need-to-know basis by job function.

Written Requests for Access Changes Required: To obtain or change access privileges, a representative of the user department should complete and sign a form that requests the specific access privileges and submit the documentation to the IT department. The IT department will then submit the form to the appropriate application owner who will approve or deny the request. The system administrator will then make the necessary changes to the access privileges for approved requests.

Segregation of Duties: Appropriate segregation of duties related to application systems will be maintained.

Control Access to Application Security Tables: Application-level access control tables and profiles (the lists maintained within a computer application that contain access authorizations) will be protected from unauthorized access. Generally, the system administrators should be the only people with access to these functions.

System Isolation: Extremely sensitive application systems will be run on dedicated and isolated processors.

Transferred or Terminated Users

Notification of User Termination/Transfer: Supervisors and managers, and the Human Resource Department will notify the IT department immediately upon the resignation, termination or transfer of employees to ensure that their access to corporate systems is revoked.

Revocation of User Credentials: All IDs and passwords will be revoked upon termination/resignation of employees and revoke/modify access upon transfer of responsibilities.

Supervisor Coordination with System Administrator: For situations where users with access to highly sensitive information are terminated, the employee's supervisor is responsible for directly coordinating with the system administrator or other appropriate supervisor to remove the user's access rights.

User Clearance Requirements: All PCs, Phones, Modems, keys, ID cards, software, data, documentation, manuals etc. of terminated personnel must be returned to the employee's direct supervisor or the Human Resource Department, as appropriate.

Inspection of Employee Materials: Information Systems shall coordinate with Human Resources to ensure that upon termination of employees, all materials that an employee wishes to remove from the premises will be inspected.

Employees Involuntarily Terminated: Information Systems shall coordinate with Human Resources to ensure that proper procedures for the removal of employees terminated for a cause will be established. Depending on the nature of the termination, the former employees will be subject to varying levels of observation and escort.

2.7 Antivirus Policy

Computer viruses are programs designed to make unauthorized changes to programs and data and can therefore cause destruction of IT resources.

Virus detection software shall be installed in all servers, laptops and desktop computers and shall be updated continuously with the latest updates available. The antivirus should be updated at least once a week.

Files on any media (removable storage media/fixed storage media) from third-party sources shall be checked with the anti-virus program before copying the files into any HAL system.

Users shall be prohibited from writing, compiling, copying, distributing, executing or attempting to introduce any program code that may damage, hinder performance and/or change a computer system or network setting.

Any program code that a user deliberately, accidentally or mistakenly distributes through any means, without the approval of the ICT shall be considered a threat to HAL's information system.

Users, including outsourced personnel, interns, contractors, and consultants shall not install any software or hardware used to circumvent HAL's information security policies.

These might include password hacking tools, decrypting tools, discovery tools, and the like. These software and hardware shall be held under strict control, and only loaded when necessary.

HAL staff suspecting a virus infection in any of HAL's computer system shall immediately report to Information technology for immediate attention and disinfections.

ICT department to install and maintain up-to-date corporate antivirus system with a centralized administration kit. The centralized administration kit shall manage all devices that have the antivirus software and push regular updates.

2.8 IT Configuration and Patch Management Policy

Overview

As HAL becomes increasingly dependent on information technology solutions to support critical processes, it also increases its exposure to security and other software vulnerabilities.

Principles

IT configuration and patch management process is part of HAL's overall security policy. All service provider agreements must contain an adequate configuration management process. Oversight and accountability is the responsibility of HAL and any contracted Service Providers.

Requirements

The following are mandated for a configuration and patch management process:

- Configuration Management
- Provides assessment of asset compliance.
- Identifies non-compliant assets.
- Creates a plan to bring non-compliant assets into compliance

Execute the plan.

The Service Provider must provide documentation that assets are in compliance to the HAL Information systems & security standards.

Patch Management

Vulnerability identification and remedies (e.g. patches): HAL or its designated service provider will proactively monitor for vulnerabilities and patches for all software identified in the system inventory.

Prioritization of Patches: HAL or its service provider must prioritize the set of known patches and provide classification to sectors, regions, and units on the criticality of each patch.

Risk assessment: When HAL or its designated service provider discovers vulnerability and a related patch and/or alternative workaround is released, then HAL or its designated service provider will consider the importance of the affected assets and/or area of operations, the criticality of the vulnerability, and the risk of applying the patch. When vulnerability is identified and no patch is available, HAL or its designated Service Provider must evaluate the risk of the

vulnerability and, based on that risk, take action to mitigate the risk through other means until a patch becomes available.

Change Control: HAL or its designated service provider will follow the standard Change Control process for application of any changes to configuration.

Assurance of Deployment: The Service Provider must provide documentation that patches have been effectively deployed to all applicable environments and/or infrastructure.

2.9 Internet and E-mail Policy

Access to the Internet is provided to HAL staff for the benefit of the company. Staff members are able to connect to a variety of information resources globally. Conversely, the Internet is also full of risks and inappropriate material. This policy will be used to ensure that all HAL staff members are responsible in the use of the internet.

Acceptable use

Staff members using HAL's Internet address are representing HAL. They are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of areas where acceptable use guidelines apply are:

- Accessing databases for information as needed.
- File downloading and uploading (File Transfer Protocol FTP).
- Remote access (SSH, VPN, Terminal services, Citrix).
- Communication tools (Email, IM, Voice and Video).
- Collaboration tools (Groove, online presentations, discussion groups, blogs, wikis, Feeds).
- Video and sound streaming.
- Access to Intranet sites, systems and facilities.

Unacceptable Use

Staff members must not use the Internet for purposes that are illegal, unethical, harmful to HAL, or non-productive. Examples of unacceptable use are:

- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
- Conducting personal business using company resources.
- Transmitting any content that is offensive, harassing, or fraudulent.
- Misusing, disclosing without proper authorization, or altering personnel information (e.g., making unauthorized changes to personnel files, or sharing personnel data with unauthorized personnel).
- Any unauthorized, deliberate action that damages or disrupts computing systems or networks; alters their normal performance, or causes them to malfunction.

- Willful or negligent introduction of computer viruses, worms or other destructive programs into company systems or networks or into external systems and networks.
- Unauthorized decryption or attempt at decryption of any system or user passwords or any other user's encrypted files.
- Packet sniffing, packet spoofing, or use of any other means to gain unauthorized access to information, a computer system, or network.
- Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization.
- Unauthorized downloading of any shareware or freeware programs or files for use without authorization in advance from the user's supervisor or team leader.
- Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violates any national or international laws, and regulations.
- Deliberate pointing or hyper-linking of institution Web sites to other Internet/WWW sites whose content may be inconsistent with or in violation of the aims or policies of the organization.
- Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls and authorization.
- Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to comments based on race, national origin, gender, sexual orientation, age, disability, religion, or political beliefs.
- Playing of games or initiating hoaxes.
- Gambling and playing games using company resources
- Accessing pornography sites.
- Accessing hacker sites, TOR websites and dark web.
- Participation in on-line contests or promotions.
- Use of Internet facilities to issue statements or opinions on any subject on behalf of organization or on behalf of other individuals unless all parties have endorsed these statements.
- Requesting, accessing, posting, or downloading of any material that incites crime or terrorism (as defined in either the receiving hosting country, or any country through which the information is routed).

Website Advertising

Third-party products or services shall not be advertised or promoted in the organization's website without prior written approval from the management. Other than that, links to external websites shall not be established without prior written approval from the management.

The content of the organization's website shall only be changed or updated by authorized personnel and sensitive in-house information shall not be posted on the organization's website.

HAL reserves the right to access the contents of any messages sent over its facilities if HAL believes, in its sole judgment, that it has a need to do so.

2.10 Audit Trails

The systems shall ensure that relevant information (an audit trail) about actions performed by users, or processes acting on their behalf can be linked back to the user and the user held accountable. The systems shall protect this audit trail from unauthorized access or modification.

The audit trail shall provide end-to-end user accountability for all security relevant events and must be traceable for the lifetime of the request or activity.

The systems shall, by default, cause a record to be written to the security audit trail for at least each of the following events (the IT Department may opt to not log some of these events due to operation constraints):

- Invalid user authentication attempts.
- Logons and activities of privileged users
- Unsuccessful data or transaction access attempts.
- Successful accesses of security-critical systems resources.
- Changes to users' security profiles, privileges, or attributes.
- Changes to access rights of resources.
- Creating new accounts.
- Changes to the systems security configuration.
- Modification of systems software.
- Modification of application software.
- Modification of data (e.g. master files / transaction files).

For each recorded event, the audit record shall identify, at a minimum:

- Date and time of the event.
- User-id and associated point of physical access, e.g., terminal, port, network address, or communication device.
- Type of event.
- Name of resources accessed.
- Success or failure of the event.
- Old Value / New Value.

Actual or attempted passwords shall not be recorded in audit trails.

Audit control data, e.g., audit event tasks, must survive systems restarts.

To optimize on system storage, audit trails shall be archived in alternative storage locations at least one per month.

The ICT Manager will actively ensure that security events are logged and monitor system activity and be aware of all aspects of the system, including what the normal load is, who has access to the system, days/times when different individuals access the system, etc.

Only the Administrators group shall have the right to manage auditing and security logs.

Network systems will be monitored to ensure conformity to access policy and standards. This is necessary to determine the effectiveness of measures adopted and to ensure conformity to an access policy model. HAL reserves the right to monitor all traffic on the HAL network. Any or all users, PCs, terminals, network addresses, user ID"s, email or other network traffic may be monitored at any time for compliance with security controls and policy.

High risk data must be encrypted during transmission over insecure channels.

Confidential data shall be encrypted during transmission over insecure channels.

Backups of data must be handled with the same security precautions as the data itself.

When systems are disposed of, or re-purposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

Denial of Service

Users will be denied service due to presence of malware on their computers which poses a threat to the rest of the organization's users and infrastructure. In these cases, users will be denied login access to their machines and emails until the problem is dealt with by IT.

Cyber security Measures

In addition to secure firewalls, Automatic Backups and Antivirus Software, the organization will invest in user training and awareness through the Cyber Security training that is mandatory to all staff. User training and awareness is a proven tried and tested method in cyber security as it empowers users to avoid security pitfalls.

2.11 Incidence Handling and Response

The following standards relating to servers apply to those residing on the enterprise network:

Employee Reporting Requirements: All employees of HAL are responsible for maintaining a familiarity with the information security policies, standards and guidelines and are responsible for reporting any suspected security breaches or violations.

Recipients of Reports: Employees who suspect a security breach or violation will communicate their concerns to their direct supervisor or other official in their supervisory chain. This individual must then evaluate the allegations and refer severe violations to the information management executive.

Timeliness of Reporting: Security breaches will be reported in a timely manner based on the severity of the incident and the nature of the data involved. Provision of Violation Information

to Owners: The information security manager is responsible for summarizing and reporting data security violations to data owners on a timely basis.

Reportable incidents: Incidents which must be reported include violations of security policies and standards by other HAL employees or contractors, and attempts to access HAL information resources by unauthorized personnel.

2.12 ICT Equipment Handling

Employees will be held liable for any loss or damage of the company's official laptop, computers, tablets and phones that are directly under their custody and therefore responsible in case of any loss or damage that occurs in and out of office.

Damage, Loss, and Theft

An employee shall report in writing any damage or loss of HAL IT property/assets under their custody to both her/his supervisor and the IT manager. The employee is held liable for any cost of repairs for any damage caused or replacement in case of loss while asset is under their custody.

The employee shall be required to immediately report to the police and obtain a police abstract for assets stolen while in their custody. The employee will submit the police abstract to the Human Resource Manager together with a full statement of circumstance leading to the theft of the asset.

3.0 PRIVACY AND DATA PROTECTION

All HAL Information is “proprietary”, that is, the property of HAL or applicable third parties that HAL has an interest in protecting wherever it exists, regardless of location or storage medium (e.g., personally owned computing equipment, third party owned computing equipment, or company devices. This information must be protected by HAL employees, and users, and service providers against unauthorized disclosure, modification, compromise, or destruction.

Protection for HAL Information is supported by implementing the concept of need-to-know. Need-to-know supports authorized access and sharing of HAL Information within and across functions for those who can demonstrate a legitimate need and obtain access approval from the Information Owner responsible for the HAL Information.

Some HAL Information is sensitive and/or could create adverse consequences if disclosed and therefore needs additional protections beyond those mandated for all HAL Information. All information resources shall be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection shall be consistent when the data is replicated and as it flows through HAL. Data owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to this classification. Three classes of classification are:

- a) **Critical/High Risk:** Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Payroll, personnel, and financial information are in this class. Other data may need to be treated as high risk because it would cause severe damage to HAL if disclosed or modified.
- b) **Confidential/Medium Risk:** Data that would not expose HAL to loss if disclosed, but that the data owner feels shall be protected to prevent unauthorized disclosure.
- c) **Public/Low Risk:** Information that may be freely disseminated.

Data custodians are responsible for creating data repositories and data transfer procedures which protect data in the manner appropriate to its classification.

3.1 Data Privacy Laws

HAL will ensure to adhere to all data privacy laws that are enacted in Kenya and internationally in order to protect all the stakeholders who share their data with HAL in the course of doing business. HAL shall maintain high levels of data abstraction to avoid personal data from being accessed by unauthorized persons. Processing of personal data shall be done with the consent of the data subject; collection, processing, storage and transmission of personal data shall be done in a lawful and non-fraudulent manner; personal data shall be collected for a specific purpose and shall not be stored for longer than is necessary; data collected must be accurate and up to date; transparency in disclosure of personal data held by a data controller; and confidentiality and security of personal data processing.

Personal Data in this case refers to any information relating to an identified or identifiable natural person". It includes, but is not limited to names, bank account information, address, medical records, personal email addresses, credit card information, photos, videos, usernames and passwords. These data may be gathered by HAL through the various ICT systems such as finance systems and HAL website.

HAL will not sell any personal data to third parties, nor will it give access to personal data to third parties. All parties sharing data with HAL reserve the right to be forgotten i.e. they can easily request for all the data shared with HAL to be deleted. HAL shall also maintain systems that enable users who subscribe to updates from the website to unsubscribe at any moment they wish to do so and that the data they used to subscribe shall be automatically deleted.

4.0 PHYSICAL AND ENVIRONMENTAL CONTROLS

All IT infrastructure and technology shall be protected by access control techniques that are appropriate for their criticality or sensitivity. Access to any HAL computer facility, IT infrastructure or technology component shall be restricted to authorized personnel only. Specifically, data centres shall be secured and access limited only to authorized personnel at all times and visitors' logs shall be maintained.

Physical security controls shall be in compliance with all local, regional, fire and safety regulations, as well as insurance requirements.

Measures shall be taken to minimize the risk of a fire from occurring within an installation, or from spreading into the installation from an adjoining area. Automatic and manual fire suppression/extinguishing systems shall be installed in computer rooms. Personnel must not be endangered by the activation of an automatic fire extinguishing system. All fire detection and fire extinguishing equipment shall be serviced and tested at the manufacturer's required intervals or as required by Governmental/local standards, whichever is the more stringent.

All Data Centers require clean, temperature/humidity-controlled air, which must meet computer manufacturer's specified temperature and humidity ranges.

All computer installations must have a dependable, consistent electrical power supply that is free from surges and interference, for all computer, air conditioning and security systems. A backup power supply shall be considered for the computer systems such as an uninterruptible power supply (UPS System).

Users must employ all reasonable means to physically secure their laptops when not in use, including using locking devices where provided. Users need to secure their laptops in the workplace, at a residence, while travelling or when left in a vehicle. Users must not access classified HAL Information in a public place, e.g. on a train, aircraft or bus if it can be viewed by others.

5.0 CHANGE MANAGEMENT POLICIES

Software Change Control covers the control of all aspects of HAL systems software including the operating system its associated packages (DBMS etc.) and utilities, third party and locally developed applications, together with any command procedures and documentation to support and run them.

Change Management aims to manage the process of change and consequently limit the introduction of errors and so incidents related to changes. The objective of Change Management is to ensure that standard methods and procedures are used, such that changes can be dealt with quickly, with the lowest possible impact on service quality. All changes should be traceable, in other words, one can answer the question, "what changed"? After recording the Request for Change (RFC), IT staff responsible for the making the change will make an initial assessment to check if any of the RFC"s are unclear, illogical, impractical or unnecessary. Such requests are rejected, stating the reasons. The person who submitted the request should always be given an opportunity to defend his or her request.

4.1 Obligations

When changes are required to systems software, associated packages and utilities, applications software, command procedures, or documentation, it is essential that the changes are:

- Appropriately authorized and approved
- Thoroughly tested
- Sufficiently documented
- Implemented at an appropriate time.

Any change must only be transferred into the production environment when approved by the appropriate System Custodian.

Sound software security management requires the procedures to manage the change control for applications and systems changes are clearly defined. There must be a set of Software Change Control Procedures to assist the process.

All operational software relating to strategic systems should be placed under appropriate Configuration Management.

4.2. Change Control Responsibilities

Specific personnel will be given the responsibility for the implementation of changes by undertaking appropriate testing in the test environment, and, subject to the appropriate approvals, moving the changes to the production environment. All elements of the system will be subject to Software Change Control Procedures.

There should be a separation of responsibilities in the transfer of software from test into the production environment. Any change request will be analyzed by an officer then tested by a different officer before implementation.

4.3. Change Control Environment

Two separate environments should be maintained for all HAL systems:

- Testing
- Production

Migration of software between environments should only be undertaken after obtaining the appropriate sign-offs as specified in the Software Change Control Procedures. New or modified software should be transferred to the Testing Environment for systems and acceptance testing by an appropriate testing group, according to an agreed test procedure.

Following successful completion of testing and approval by the appropriate systems custodian, the new or modified software should be transferred to the Production Environment for implementation under the control of its Operations staff. A contingency plan to enable the software to be restored to its previous version in the event that the implementation is unsuccessful should be prepared where appropriate.

4.4. Documentation

The following documentation must be maintained;

Software Change Request

No software change is to be undertaken without appropriately authorized software Service Request. The Service Request is also the principal documentation to be completed for the software change management process.

Technical, Operations and End User Documentation

Appropriate documentation in respect of each software change must be completed in sufficient detail and accepted before the change is implemented in the production environment.

The following guiding principles should be applied in change management: -

- **Impact Assessment, Prioritization and Authorization** - Assess all requests for change in a structured way to determine the impact on the operational system and its functionality. Ensure that changes are categorized, prioritized and authorized.
- **Emergency Changes** - Establish a process for defining, raising, testing, documenting, assessing and authorizing emergency changes that do not follow the established change process.
- **Change Status Tracking and Reporting** - Establish a tracking and reporting system to document rejected changes, communicate the status of approved and in

process changes, and complete changes. Make certain that approved changes are implemented as planned.

- **Change Closure and Documentation** - Whenever changes are implemented, update the associated system and user documentation and procedures accordingly.
- **Training** - Train the staff members of the affected user departments and the operations group of the IT function in accordance with the defined training and implementation plan and
- associated materials, as part of every information systems development, implementation or modification project.
- **Test Plan** - Establish a test plan based on organization wide standards that define roles, responsibilities, and entry and exit criteria. Ensure that the plan is approved by relevant parties.
- **Implementation Plan** - Establish an implementation and fallback/back out plan. Obtain approval from relevant parties.
- **Test Environment** - Define and establish a secure test environment representative of the planned operations environment relative to security, internal controls, operational practices, data quality and privacy requirements, and workloads.
- **System and Data Conversion** - Plan data conversion and infrastructure migration as part of the company's development methods, including audit trails, rollbacks and fallbacks.
- **Testing of Changes** - Test changes independently in accordance with the defined test plan prior to migration to the operational environment. Ensure that the plan considers security and performance.
- **Final Acceptance Test** - Ensure that business process owners and IT stakeholders evaluate the outcome of the testing process as determined by the test plan.
- **Post-implementation Review** - Establish procedures in line with organizational change management standards to require a post-implementation review as set out in the implementation plan.

5.0 ASSET MANAGEMENT

5.1 Copyrights and License Agreements

It is HAL's policy to utilize firm approved and supported software and hardware, upgrade and maintain software and hardware, manage and maintain an inventory of owned assets and comply with all laws regarding software licensing and intellectual property. This directive applies to all software that is owned by HAL, licensed to HAL, or developed using HAL resources.

IT Department will:

- Label all HAL's IT assets
- Maintain inventory records.
- Periodically scan HAL's computers to verify that only authorized software is installed.
- Ensure that all licenses are valid and renewed upon expiry.
- Safeguard hardware and data.
- Account for IT assets and configuration items.
- Verify configuration records
- Maintain logical and physical security.
- Ensure there is no use of unauthorized and illegal duplication of software.

For all assets, owners should be identified and the responsibility for the maintenance of appropriate controls should be assigned. The implementation of specific controls may be delegated by the owner as appropriate but the owner remains responsible for the proper protection of the assets. Through asset management, the IT function should account for IT assets and configurations, verify the configuration records and correct exceptions and provide accurate information on configurations and the referring documentation as well as a sound basis for other processes (incident, problem, change and release management).

Data owners will:

- Classify assets.
- Implement specific controls for protection of assets.

5.2. Acquisition Guidelines

Procurement Control

HAL utilizes centralized procurement system. The IT function is to provide specifications to acquire IT-related infrastructure, facilities, hardware, software and services needed by the business.

Software Acquisition Guidelines

The Information Technology department must be notified of all new software requirements and installations. The IT department reserves the right to refuse software if it presents any risk to the company.

There are 3 types of software available to HAL employees:

Pre-approved Purchase Software: Software, generally shrink-wrapped and commercially marketed, developed by an organization outside of HAL. HAL IT Department maintains a current list of these titles.

Specialized Purchase Software: Software developed by a vendor to perform a unique function that cannot be accomplished using pre-approved purchase software. This software requires a capital appropriation and the System Administrator's approval.

In-house Developed Software: An application or system designed specifically by and for HAL. Prior to development of a system, the System Administrator must be contacted to determine if similar systems can be utilized to fulfill requirements and no duplication of effort is involved. All HAL development standards must be followed.

Prior to the selection of the second or third option, the System Administrator must participate in a build versus purchase analysis that is based on the total inventory and resource of systems within HAL.

All security software shall be selected by the Information Technology and Internal Audit departments. Any new operating system or operating environment must be approved by IT Department prior to acquisition.

Hardware Acquisition Guidelines

Acquisition of PC hardware is centralized. This provides a clear approach to ensuring that HAL's interests are best served with PC hardware purchases

All signed requests associated with a specific purchase for personal computer equipment must be forwarded to the System Administrator for further processing and ordering, regardless of the associated dollar cost. This shall be subjected to the tender committee rules and regulations ruling at the time. The System Administrator must review any type of personal computer equipment purchase, including Local Area Networks (LAN), Laptops, PCs, regardless of the use and title of the system. When the user is transferred or terminated, the PC inventory is verified as part of the exit procedure by the IT Department.

During PC maintenance, the user shall be cautioned that under certain repair situations sensitive data would be vulnerable. This condition occurs when there is a failure of a hard disk necessitating its removal and replacement. If a hard disk must be removed because of problems, the user or a technician shall attempt to perform a low level format, which will erase all the information. If a low level format cannot be performed successfully, then the damage to the disk is usually extensive and consideration shall be given to physically destroying the media. Encryption will also provide protection to ensure that data is not retrievable during a repair situation.

All repairs and maintenance shall be carried out by HAL authorized ICT personnel only. At no point should employees engage the services of external ICT technicians for HAL issued hardware. All ICT assets issued by HAL i.e. hardware and installed software are the sole

property of HAL and all repairs, maintenance and troubleshooting must be carried out by HAL authorized ICT personnel.

5.3. Disposal Guidelines

All obsolete and damaged equipment will be replaced with new equipment with the guidance of the ICT department. The ICT department is the one solely charged with the responsibility of declaring equipment obsolete or irreparable. Obsolete equipment can be disposed of through sale or donation to deserving institutions through CSR.

Before disposal of any HAL equipment all data must be wiped out or deleted. Any media containing sensitive data can be physically destroyed. The same will apply to equipment that is damaged or faulty and can no longer be used for any application.

Assets register

An assets register will be maintained for all HAL software, software licenses and hardware devices. This register will be updated when any of this assets is acquired or disposed and will be reviewed on a monthly basis to ensure that it remains accurate.

6.0 BUSINESS CONTINUITY MANAGEMENT POLICIES

Overview

Disaster recovery is a proactive planning process to manage the potential loss of HAL Information or inability to access HAL Information in the event of a disaster. Disasters may be immediate, significant, and obvious, or they may be more insidious and negatively impact HAL over a period of time. The focus of disaster recovery and business continuity is the protection of HAL Information stored within HAL computing and communication resources. As HAL becomes more dependent on its computer and communications resources, the loss of these resources could cripple the operations of the company and lead to loss of revenue.

6.1. Backup Policy

- **Software:** All server software, whether acquired off-the-shelf or developed in-house or created personally should be backed up weekly.
- **System data:** System data is to be backed up at least once a week.
- **Application data:** All application data should be backed up using daily incremental backups and weekly full backups.
- **User data:** All user files will be backed up on a weekly basis. Personal files stored in user PCs will be not eligible for the company backup procedures.
- **Backup Software:** All machines will have automatic backup software installed that backups all documents on a daily basis. IT shall notify by mail all users whose machines have not backed up in any given week.
- **Storage:** All backup media must be stored in a safe and secure location away from the company's data center. All backup media must be stored in a fireproof safe. All software full backup and monthly backup media must be stored in an off-site backup archive storage location. The company will adopt modern IT user and system backup options such as cloud storage which are readily available through external vendors.
- **Data Retention:** As per the Laws of Kenya electronic records will be retained for 7 years before they are deleted.

6.2. Media Storage

For safety, all backup media & data shall be stored offsite and will be accessed for the purpose of restoring data as part of business continuity.

6.3. Restoration of Data

The restoration of data using data backups must be tested at regular intervals (a minimum of once a quarter is recommended) and at least after every modification to the data backup procedure. It must at least once be proven that complete data restoration is possible (e.g. all data contained in a server must be replicated on an alternative server using substitute

reading equipment to the data backup writing equipment). This ensures reliable testing as to whether:

- Data restoration is possible.
- The data backup procedure is practicable.
- There is sufficient documentation of the data backup, thus allowing a substitute to carry out the data restoration if necessary.
- The time required for the data restoration meets the availability requirements.

6.5. Disaster Recovery

Disaster Recovery Planning (DRP) is the preparation and testing of plans to recover from a disaster. DRP supports HAL's overall plan to ensure the continuity of the total operations in the event of a disaster. The detailed contents of the DRP will depend on the nature and criticality of the systems (those applications / systems that support critical operations) described the value and sensitivity of HAL Information involved, and the potential impacts resulting from identified threats. The DRP must provide a complete, consistent, and practical statement of all actions, roles, and responsibilities, prior to, during, and after a disaster to:

- Ensure minimum disruption to the performance of the affected business unit while allowing HAL to function;
- Reinstall HAL computing and communication resources based on the stated priority order within time limits specified by HAL management.

The DRP must include:

Based on the Business Impact Analysis (BIA), the functional Units and IT Team will work together to classify the application based on the Recovery Time Objective (RTO). The Business Impact Analysis or BIA will navigate you to the negative impact on performance if HAL's computing and communication resources are lost or unavailable for varying periods.

Back-up requirements for HAL Information based on the maximum tolerable downtime and Recovery Time Objective (RTO) of HAL computing and communication resources as defined by management.

Prioritization and capability for the order of recovery of HAL computing and communication resources, including the re-entry of any lost HAL Information and the order of recovery if the disaster impacts multiple units at one site. A Disaster Recovery (DR) Classification has to be determined and maintained for all HAL Applications.

Methodology for communications to employees and service providers to execute the DRP.

Ongoing DRP maintenance and testing to include:

Plan maintenance formally documented and kept up-to-date at all times. Testing strategy reviewed and tested at least annually. Testing specifications must be documented and include specific objectives, metrics, schedules, time frames, scenarios, audit logs, sign-off by users and business processes to support the business in the interim prior to the recovery and feedback for improvement.

7.0 Incident Management

Incident Management is a reactive task, i.e. reducing or eliminating the effects of actual or potential disturbances in IT services, thus ensuring that users can get back to work as soon as possible after an incident has occurred. For this reason, incidents are recorded, classified and allocated to appropriate IT specialists; incident progress is monitored; and incidents are resolved and subsequently closed. The IT department will be required to use a service desk system to record and track all incidents reported by users. This system will generate tickets for incidents reported and tracking them until they are resolved or closed.

In this context, 'Incidents' include not only hardware and software errors, but also service requests. Service requests can be made for services that are agreed to be provided under SLA's and are delivered through agreed procedures which have appropriate checks and controls and where records are maintained.

The following guidelines apply for incident management;

- **Employee Reporting Requirements:** All employees of HAL are responsible for familiarizing themselves with the information security policies, standards and guidelines and are responsible for reporting any suspected security breaches or violations.
- **Recipients of Reports:** Employees who suspect a security breach or violation will communicate their concerns to their direct supervisor or other official in their supervisory chain. This individual must then evaluate the allegations and refer severe violations to the information management executive.
- **Timeliness of Reporting:** Security breaches will be reported in a timely manner based on the severity of the incident and the nature of the data involved.
- **Provision of Violation Information to Owners:** The information security manager is responsible for summarizing and reporting data security violations to data owners on a timely basis.
- **Reportable incidents:** Incidents which must be reported include violations of security policies and standards by other HAL employees or contractors, and attempts to access HAL information resources by unauthorized personnel.

Subsequent to resolution of major incidents, IT should carry out a root cause analysis to identify what caused the incidence and ensure that it has been fully resolved.

7.1 Reporting of Security Violations

- **Employee Reporting Requirements:** All employees of HAL are responsible for maintaining a familiarity with the information security policies, standards and guidelines and are responsible for reporting any suspected security breaches or violations.

- **Recipients of Reports:** Employees who suspect a security breach or violation will communicate their concerns to their direct supervisor or other official in their supervisory chain.
- **Timeliness of Reporting:** Security breaches will be reported in a timely manner based on the severity of the incident.
- **Provision of Violation Information to Owners:** The IT manager is responsible for summarizing and reporting data security violations to data owners on a timely basis.
- **Reportable incidents:** Incidents which must be reported include violations of security policies and standards by other HAL employees or contractors, and attempts to access HAL information resources by unauthorized personnel.

7.2 Network Security Monitoring

1. **Purpose of Monitoring:** Systems will be monitored to ensure conformity to access policy and standards. This is necessary to determine the effectiveness of measures adopted and to ensure conformity to an access policy model.
2. **Company Authority to Monitor:** HAL reserves the right to monitor all traffic on the HAL network. Any or all users' PCs, laptops, network addresses, user ID's, email or other network traffic may be monitored at any time for compliance with security controls and policy.
3. **Publication of Monitoring Policy:** To maximize the effectiveness of auditing, unit managers will publicize the fact that it is HAL policy to audit network activity.
4. **Authorization of Monitoring Activities:** Company management must formally authorize all monitoring activities.
5. **Control of Network Monitoring Devices:** Only authorized personnel can use network diagnostic test hardware and software such as sniffers and monitoring devices to monitor traffic on the HAL network. Information owners should be notified when non-routine network monitoring devices are used to monitor their data.
6. **Monitoring of System Use:** Unit managers will implement procedures for monitoring system use. Such procedures are necessary to ensure that users are only performing processes that have been explicitly authorized. The level of monitoring required for individual systems will be determined by a separate risk assessment. Areas that will be considered are:
 - Login and access attempts
 - Review of logon patterns for indications of abnormal use or revived user IDs.
 - Allocation and use of accounts with a privileged access capability.
 - Tracking of selected transactions.
 - The use of sensitive resources.
 - Dial-up activity.
 - Firewall activity.

- OS and application access attempts.
 - Security administration activity
- 7. Audit Trail Rules:** Audit trails recording exceptions and other security-related events should be produced and kept for an agreed upon period to assist in future investigations and access control monitoring. A record of rejected access attempts will be created. At a minimum, audit trails will include:
- User IDs.
 - Dates and times of access
 - IT resources or systems accessed
- 8. Audit Trail Retention:** Audit trails recording exceptions and other security-related events should be maintained in accordance with HAL record retention policies.
- 9. Use of Audit Tools/Aids:** The use of automated tools to facilitate review audit data on a frequent basis is strongly recommended. Additionally, to ensure the accuracy of audit logs, system clocks should be synchronized across the network.
- 10. Role of System Administrator:** For applications that have been determined to contain sensitive information, and where the system or application software permits, the system administrator will produce security log reports, investigate access violations and resolve the violations periodically, as determined by the information owner.
- 11. Internet Access Monitoring:** An audit log of Internet access transactions will be implemented and maintained by ICT Managers. Employees will be advised that they should have no expectation of privacy with regard to computer equipment, information, software, etc. At any time and without prior notice, HAL management reserves the right to examine E-mail, personal files and other information stored on HAL information resources.
- 12. IS Monitoring of Firewall Audit Reports:** The IT department will review the Internet connection audit reports created on the firewall for any unusual activities, and will notify Internet Operations in the event such activities are detected. The period between reviews must not exceed one (1) week. Alarms must be in place to alert system administration personnel about security or other related events generated from the firewall. This should be performed real-time using existing SNMP or other network monitoring tools. Events to be monitored include:
- Behavior in violation of HAL information security policies and standards
 - A new host/device joining the network
 - Emergence of a new MAC address on the network
 - Known hosts not responding to user requests
 - Well known hacker signatures
- 13. IS Monitoring Reviews:** Unit Management are responsible for establishing periodic security monitoring review schedules to detect unauthorized attempts to access HAL computers.

7.3 Use of Intrusion Detection Systems

Requirement for Use of Intrusion Detection Systems: The use of intrusion detection systems to perform real-time analysis of network traffic patterns to detect attempted attacks is required for web-based connections and for use within the internal network. Without intrusion detection software or hardware it is more difficult to detect attempts to breach security, as well as certain types of sophisticated attacks, thus increasing the likelihood of undetected compromise of system integrity and confidentiality.

Real-time Intrusion Detection on Public Access Systems: Firewalls must utilize system monitoring tools that provide real-time alerts whenever suspicious user activity is detected.

Response to Intrusions/Attempts: Unauthorized attempts (either successful or unsuccessful) to access or modify data protected behind the firewall will be promptly investigated by system administration and information security personnel.

7.4 Compliance Monitoring

- **IS Compliance Review Program:** The ICT Manager in liaison with the unit management is responsible for establishing a program to continually monitor the HAL system security environment for compliance with published information security policies, standards, and procedures. This will include an assessment of user practices, operations, and systems configurations.
- **Supervisor Role in Compliance Monitoring:** Supervisors will continually monitor the practices of HAL employees and consultants under their control to ensure that a high level of compliance with security policies and standards is maintained.

8.0 IT HUMAN RESOURCES

HAL will maintain IT personnel recruitment processes in line with the overall organization's human resource policies and procedures (e.g., recruitment, onboarding, promotions, termination etc.). The company will implement these processes to ensure that the company has appropriately deployed IT workforce with the skills necessary to achieve organizational goals.

Evaluate staffing requirements on a regular basis or upon major changes to the business, operational or IT environments to ensure that the IT function has sufficient resources to adequately and appropriately support the business goals and objectives.

Personnel Competencies - Regularly verify that personnel have the competencies to fulfil their roles on the basis of their education, training and/or experience. Define core IT competency requirements and verify that they are being maintained, through in-house training and certification courses, where appropriate.

Staffing of Roles - Define, monitor and supervise roles, responsibilities and compensation frameworks for personnel, including the requirement to adhere to management policies and procedures, the code of ethics, and professional practices. The level of supervision should be in line with the sensitivity of the position and extent of responsibilities assigned.

IT Staff Training - Provide IT employees with appropriate orientation when hired and ongoing training to maintain their knowledge, skills, abilities, internal controls and security awareness at the level required to achieve organizational goals.

Dependence Upon Individuals - Minimize the exposure to critical dependency on key individuals through knowledge capture (documentation), knowledge sharing and succession planning.

Staff Clearance Procedures - Include background checks in the IT recruitment process. The extent and frequency of periodic reviews of these checks should depend on the sensitivity and/or criticality of the function and should be applied for employees, contractors and vendors.

Employee Job Performance Appraisal - Require a timely evaluation to be performed on a regular basis against individual objectives derived from the company's goals, established standards and specific job responsibilities. Employees should receive coaching on performance and conduct whenever appropriate.

Job Change and Termination - Take expedient actions regarding job changes, especially job terminations. Knowledge transfer should be arranged, responsibilities reassigned and access rights removed such that risks are minimized and continuity of the function is guaranteed.

Contracted Staff - Ensure that consultants and contract personnel who support the IT function know and comply with the company's policies for the protection of the company's information assets such that they meet agreed-upon contractual requirements.

9.0 CONCLUSION

The policy has been developed to establish information technology guidelines that will integrate and govern the use of ICT into HAL operations for effective service delivery. The policy, together with the company's ICT Strategy and structure will address the need to transform HAL into a more effective and efficient institution through the adoption and implementation of best practices.

10.0 MONITORING AND EVALUATION

The Information Communication Technology Policy is the responsibility of the Information Technology Manager. These policies will be reviewed and evaluated and updated annually to match the changes within the company and also changes in technology and the environment in which HAL operates in.

Updates may include the creation of new policies, modifications to existing policies, and/or the deletion of line item details. Updates can be triggered by several events including but not limited to new technology, security upgrades, changes in legal, regulatory, or reporting requirements, physical or environmental alterations, changes in business demands and requests from service providers.

11.0 APPROVAL

This Information Technology policy for has been approved and issued under the signature of:

.....

Managing Director
Home Afrika Limited

.....

ICT Manager
Home Afrika Limited

12.0 APPENDIX

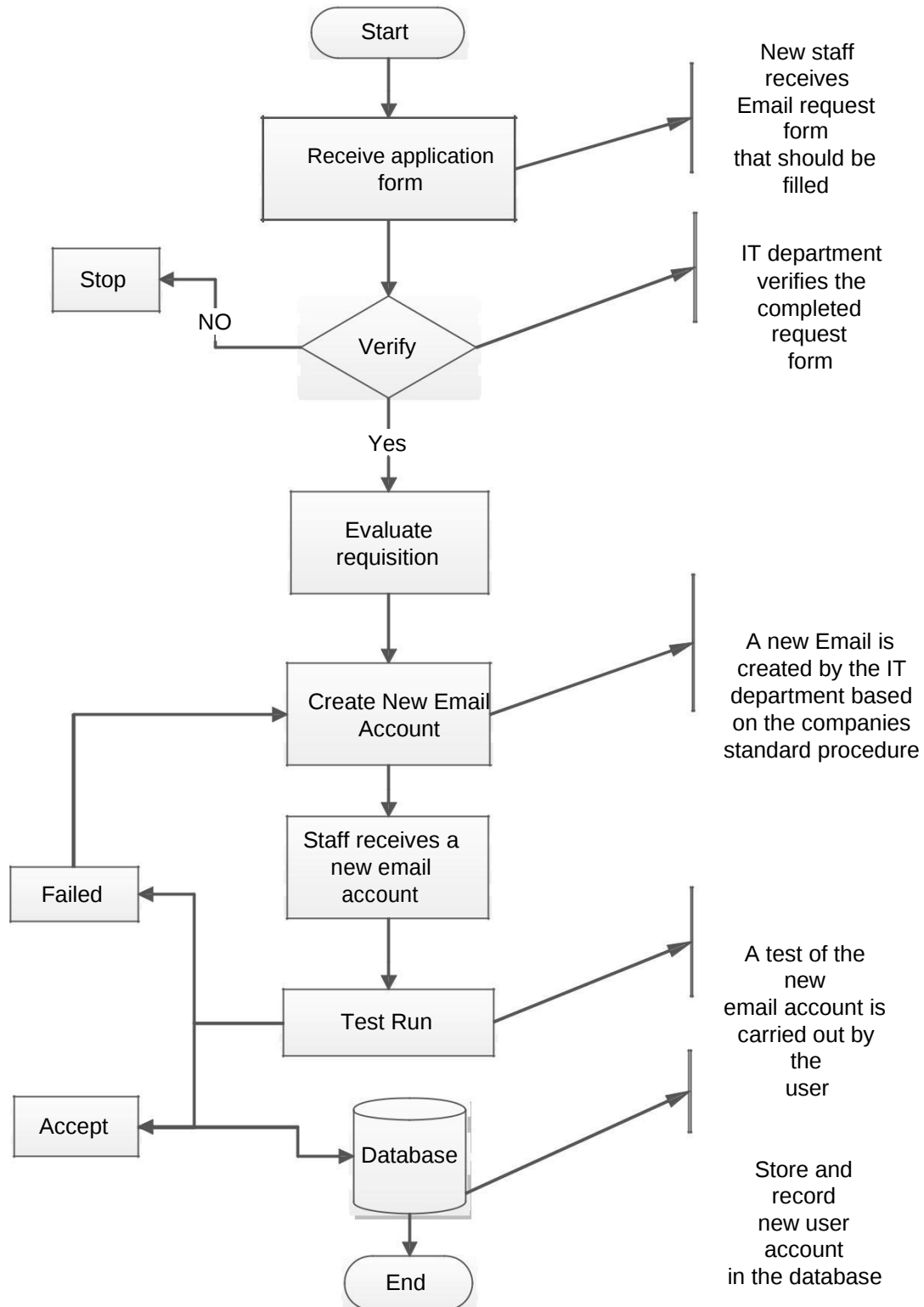
12.1 Appendix I

Equipment Liability Form

1. Staff Name
2. Department
.....
....
3. Details of the equipment/SN.....
Date Taken.....
Date of return.....
Signature
Head of IT
Approved/Not Approved
Signature Date.....
In case of any loss or damage of the said equipment, the holder will bear full responsibility.

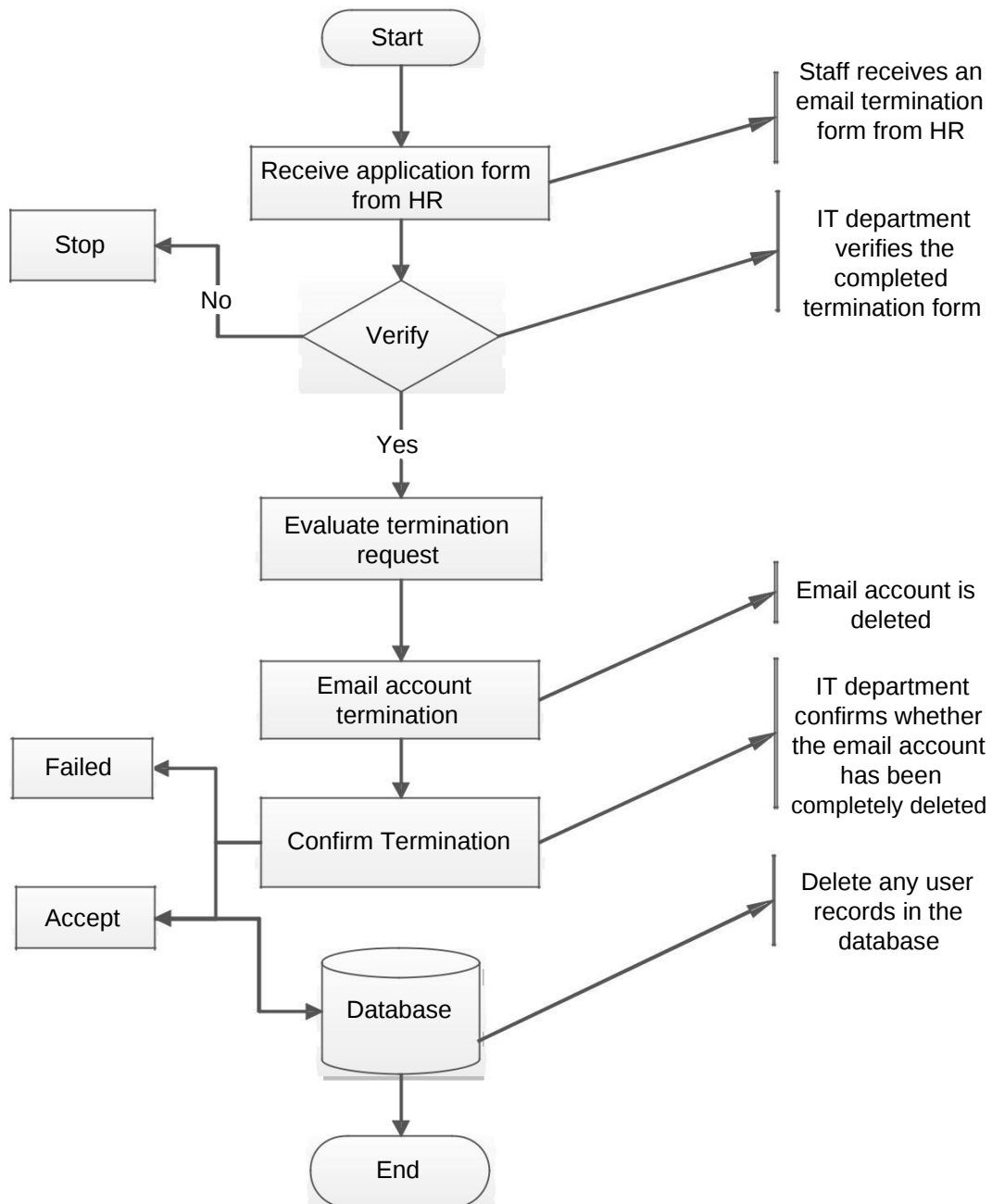
12.2 Appendix II

Email Process Flow Chart



12.3 Appendix III

Email Termination Process Flow Chart



12.4 Appendix IV

INFORMATION TECHNOLOGY USER DECLARATION AGREEMENT

Access to information technology resources and services has been granted to me as a privilege for performing job duties and responsibilities.

I have read and agreed to abide by the policies and procedures which govern the use of these services:

COMPUTER, E-MAIL AND INTERNET ACCEPTABLE USAGE STATEMENT POLICY

I will refrain from manipulating company systems, bandwidth misuse, and misuse of company resources for personal work and irresponsible use of any other information technology resources. I will also report to management any information received or obtained to which I am not entitled to and observations of attempted security violations or illegal activities.

By signing this agreement, I certify that I understand and accept responsibility for adhering to the policies and procedures referred to above. I acknowledge my understanding that any misuse on my part may result in disciplinary action including, but not limited to termination of my access privileges.

Employee Name: _____

Signature: _____

Date: _____

Head of Department:

Name: _____

Signature: _____

Date: _____

12.5 Appendix V

IT Declaration Agreement Flowchart

