OLYMPIA CAPITAL HOLDINGS PLC

INFORMATION COMMUNICATIONS AND TECHNOLOGY POLICY

Olympia Capital Holdings Plc

Information Communications and Technology Policy

Drawn by:

Secplus Consulting
Certified Public Secretaries (Kenya)
Accredited Governance Auditors (Kenya)

TABLE OF CONTENTS

1. Introduction

1.1. Purpose

It has been demonstrated that information and technology management is a vital component of any business and, when planned and managed properly, improves services to customers and suppliers, increases productivity, and reduces costs to the company.

This document aims to provide a policy framework within which Olympia Capital Holdings Plc (hereinafter "OCHL") can maximize information and technology use. Specifically, it:

a. Defines authorities, responsibilities, and accountabilities for information and technology management; and

b. Establishes policies, technological standards, and guidelines for the management of information and technology activities related to: (i) Data and Information management, (ii) Information technology management, including IT acquisition, (iii) Systems Security, (iv) Networking, and (v) Communications.

1.2. Scope

This document applies to OCHL, its subsidiaries, departments, and individuals, hereinafter jointly and severally referred to as OCHL.

1.3. Role and Functions of the ICT Department

The ICT department will undertake the following roles and responsibilities namely: -

i) Developing, maintaining, and enforcing system policies, procedures, and guidelines,

ii) Developing Information Management Systems, architecture and infrastructure,

iii) Running an effective and efficient support and maintenance services department,

iv) Systems administration, and

v) Managing connectivity issues between branches and the outside world.

1.4. Department Authority, Responsibility and Accountability

OCHL leaders and supervisors have the authority, responsibility, and accountability for:

i) Managing their departmental information resources, and ensuring that sound information management practices are followed;

ii) Ensuring that the delegated responsibility for information technology is carried out fully;

iii) Ensuring compliance with the policies and standards associated with this chapter;

iv) Ensuring all equipment is returned when an employee leaves OCHL;

v) Developing staff to make effective use of information technology; and

vi) Ensuring that information technology plans address human resource requirements in terms of job design, training, and working environment.

2. Computer Equipment and Networks

2.1. General

All computer equipment purchased with OCHL funds belongs to OCHL. It is the user's responsibility to keep it secure and in good working condition and to report any hardware or software defects or faults to the OCHL ICT department promptly.

2.2. Transfer of Equipment to Users

Upon hiring a new employee or upon acquiring new computer equipment, the ICT department will ensure that the equipment being acquired or transferred to the user is captured in the equipment authorization form, appropriately tagged, and entered into the fixed asset system by Management Accounts.

The ICT department and the user should sign transfer forms associated with the old and new equipment, which will contain the following details: (a) Equipment Make and Model, (b) Serial number of equipment(s), (c) Components, (d) System specifications e.g., memory, capacity, and speed, (e) Issues, if any when the equipment is not new.

See Appendix A9 – Equipment Authorization Form

2.3. User Leaves OCHL

Upon resignation or termination from employment at OCHL, the user will surrender all computing equipment to their Department Head or supervisor. These managers should then verify that all the equipment on the equipment authorization form has been returned and should sign the form denoting the same.

Missing equipment will be valued by the ICT department and deducted from the user's final paycheck. ICT will decide the new recipient of the returned equipment. Any unallocated equipment should be submitted to the ICT department for storage and/or disposal. See the complete policy in section 16 below.

2.4. Access to OCHL Computing Equipment

Use of OCHL computing equipment is restricted to OCHL staff members only. Unauthorized persons should not have access to OCHL computer equipment unless prior arrangements with management have been made and **confirmed in writing**.

As a general rule, any damage arising from unauthorized use shall be charged directly to the OCHL employee who had been allocated that equipment.

2.5. Other Hardware

OCHL provides a wide variety of hardware, including desktop and laptop computers, printers, networking equipment, projectors, scanners, screens/monitors, and external hard drives for use by OCHL departments and personnel. The ICT department administers these resources and the policy is:

i) All hardware is to be used only for legitimate OCHL business,

ii) All hardware availed to users will meet the then-current minimum OCHL standard to facilitate support,

iii) System access by users is granted only on assigned hardware. Any other access must be duly authorized by the employee's supervisor and the ICT department,

iv) Priority for hardware may be granted to certain users or certain groups of users in support of OCHL's business needs,

v) The ICT department will take reasonable steps to ensure its hardware is free from viruses and other destructive threats to maintain the proper functioning of computer and networking hardware. Users share the responsibility for protecting OCHL hardware, and

vi) Maintenance of the hardware may be carried out by in-house ICT staff or by approved contract maintenance companies, as considered appropriate by the ICT department.

2.6. Network Authorization

The Department Head or their designated representative should promptly provide ICT with names and details of new staff members (including contract employees, interns, and temporaries) for Network account creation.

The following details should be provided: -

i) Username, company, and department,

ii) Application forms specifying specific network access and the level of access,

iii) Date of employment and termination, if known – (applies to temporary employees),

iv) Accesses required,

v) Any other privileges that should be given to that employee e.g., email or shared resources, etc., and

vi) Authorization for internet access and use.

The ICT department shall grant designated users reasonable access rights to the Network based on the above details, the authorizations of the departmental head, and in consultation with the Group Finance Director (GFD) when confidentiality and/or segregation of duty issues are anticipated. The same process shall apply to all shared resources i.e., printers, network folders, and application groups.

See Appendix A6 and A3 Email and Internet Connection Request Form and Access Form respectively.

2.7. Network Account Policy

OCHL shall define the minimum Network Account protocols that will be adhered to when creating new user accounts with respect to:

i) Usernames;

ii) Passwords, i.e., Password Strength, Password Age, Password Uniqueness, Password Change

iii) Account Locks/Lock-out duration;

iv) Log on hours;

v) Change of Account; and

vi) Change of network account protocols.

2.8. Internet, Email and Browsing

To assist in keeping OCHL computers running effectively and efficiently, and to ensure that maximum network capacity is available for everyone to work, the following general policies regarding the security and operation of the OCHL computer network apply:

i) Use of OCHL network and information resources for non-business purposes should be minimized by limiting personal e-mail and internet traffic, particularly during regular working hours. Such rights can be withdrawn at the discretion of management if one is suspected of misuse.

ii) Any employee who illegally secures internet access without approval will receive a minimum of a first and final warning letter.

iii) Downloading software/content from the internet that is not licensed to OCHL, verified, approved, or supported by OCHL business is prohibited.

iv) Use caution in opening e-mails from unknown sources. Immediately delete suspicious messages, leaving the attachment unopened. Immediately notify the ICT department. Even though your computer is protected by anti-virus software, the threat of a virus attack still exists.

v) Non-business-related high-volume traffic over the network that hinders colleagues in their use of business applications is prohibited. Examples include: -

a) Internet radio station or similar access,

b) Software downloads,

c) Audio and video downloads or real-time streaming media,

d) Excessive personal email attachments and downloads, and

e) Distribution of hoaxes, chain letters, or advertisements over the network.

vi) Users, with permission, accessing the network, email, or the Internet, using their own equipment, will be required to have up-to-date and OCHL-approved anti-virus protection.

vii) Any user who requires an e-mail account or internet access must seek written authorization from his/her respective Department Head. ICT will then use a process to allocate and maintain e-mail accounts and Internet access. Each user will have a unique username and password as described above.

2.9. General System Access Guidelines

Below are some general guidelines for the use of OCHL network resources: -

i) Boot passwords are required on all PCs and laptops. This is especially important in the case of laptops that move outside the offices.

ii) Users must neither disclose their password to anyone nor should use anyone else's password. Passwords should not be written down or easily guessed.

iii) Employees will be liable for any misuse resulting from failure to protect their password/username.

iv) Unique usernames will be allocated by the system administrators. Wherever possible, these should be consistent across applications.

v) Access levels will be determined by systems administrators and supervisors for each application.

vi) Terminals/PCs should not be left "logged in" when unattended. Where this is unavoidable, ensure that either an authorized screensaver with a password or five-minute time-out facilities is in operation. If you know you are leaving your desk for any period, you should "lock" your workstation.

vii) Unauthorized screensavers are not permitted as they can cause unacceptable overloading of PCs and the network.

viii) The System Administrator must be promptly notified of all terminations or other departures to permit the timely removal of all access rights.

2.10. Access to Software Business Applications

OCHL shall from time to time specify such applications that will comprise the Company's IT systems installed to manage information for OCHL. Access to these systems shall be granted on an "as needed" basis as per the recommendation of the respective Department Head, in consultation with the ICT Department Head and the system owner.

If the software has in-built security features, then the ICT Systems Support analyst shall have the responsibility to set up the appropriate accesses to that software.

Login names, passwords, and granted permissions provided to users shall not be shared with others. Users take full responsibility for the use, misuse and execution of their login-name, password and permissions. Users are subject to dismissal for misuse or password sharing.

2.11. Access to Shared Network Resources

These will include printers, shared drives, and other shared resources on the network. Network resources will be installed on the network for sharing among users in the same department or physically located within the same area. Authority to access such resources should be granted by the Systems Administrator or such person so designated in the ICT department, after obtaining permission from the owner of that shared resource.

Users will be subject to dismissal for misuse or unauthorized sharing of these resources.

2.12. Network Folders

All users shall be granted access to the central file server for file storage. The disk space allocated should only be used as a secondary storage space or as a backup to the local drive and limited to OCHL official information. Personal data should not be stored in the server unless the ICT Department Head, in consultation with the GFD, gives such authority. The limit to the space available to the users will from time to time be determined by ICT and shall depend on the availability of disk space in the designated file server.

The folders where such space is created will contain the username for easy identification and shall be created during user account creation. It is recommended that all users save their information in these folders for backup purposes.

The ICT department will not be held responsible for the loss of information stored on the local drive of a PC or Laptop. The department only does network file backup, unless otherwise stated.

2.13. Anti-Virus Update Procedures

OCHL shall cause anti-virus updates to be maintained centrally or separately and client scans shall be automatically handled and centrally administered by the server.

2.14. Access to the Computer Room

Physical access to the computer room or cabinet (file servers and network communication equipment) at any OCHL site is restricted to authorized computer staff. The server room or cabinet will be locked at all times and where necessary lockable racks will be used.

3. Computer Replacement

3.1. Computer Replacement Criteria

All computers should have the capacity to run standard and licensed OCHL software products. ICT will keep a separate register for all computers detailing their capacities, which will be used to determine the need for replacement. Any computer that does not meet the above standards should be replaced unless assigned to other purposes.

Due to technology changes, **any computer that is over four (4) years old** will be classified as obsolete and should be replaced, funds permitting. The same should apply to a computer that has suffered irreparable damage.

3.2. Disposal of Computers

All replaced computers should be returned to the ICT department for storage under the supervision of the ICT Department Head and then disposal following OCHL policy on technology asset disposals.

4. Procurement

The following shall be observed before and after purchasing computer-related items.

i) The user's departments will initiate computer requirements using the Purchase Requisition Form.

ii) The ICT department will analyze the required needs and develop a recommended solution.

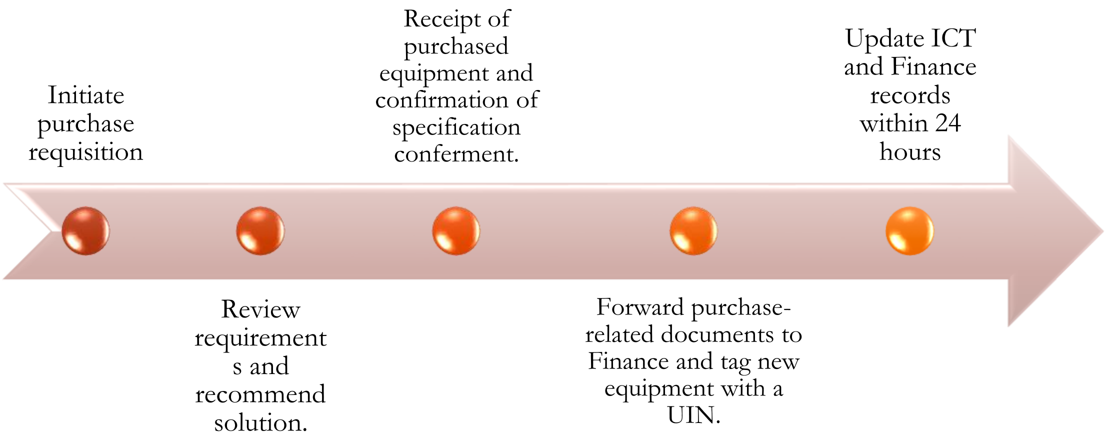
iii) If the proposed solution is acceptable, the process will commence according to the procurement procedures defined in the Finance Procedures and Policy Manual.

iv) On delivery of the equipment, ICT will ensure the supplied product meets the specifications requested.

v) All purchase-related documents should immediately be forwarded to the Finance department for recording and retention.

vi) All additions shall be appropriately tagged with a unique identification number.

vii) The asset register should be of receiving any new item. This will ensure that both the ICT and Finance department records are updated.


Initiate purchase requisition
Review requirements and recommend solution.
Receipt of purchased equipment and confirmation of specification conferment.
Forward purchase-related documents to Finance and tag new equipment with a UIN.
Update ICT and Finance records within 24 hours

5. Computer Insurance

Insurance of computer equipment will be in line with OCHL Computer equipment insurance coverage managed by the Finance Department. The ICT department will notify the Chief Accountant (or whoever is responsible for insurance matters in the Finance department at the time) of new items received for purposes of updating the Insurance Company on a monthly basis.

6. Software Licensing

All software in use on any OCHL computer should have the proper licenses as issued by the software manufacturer. OCHL's Legal Officer (original) and ICT department (photocopy) should keep copies of such licenses. OCHL's ICT Department Head must grant written permission before non-standard software is loaded onto OCHL computers.

7. Software Maintenance and Upgrades

Software upgrades and patches will be made following OCHL's standard software policy as may be updated from time to time or authorized by the ICT department. The software upgrades must be formally licensed to OCHL.

Any software installation on a user's personal computer must be done by the ICT department. These installations **should be approved in writing by the user's Department Head**.

No software other than the standard software outlined below should be maintained on the user workstations and installation of such software on OCHL computers is prohibited. Such software, if discovered by the ICT department, will lead to disciplinary procedures being taken on the user.

8. Standard Software

All software to be used by OCHL should meet the standards as set by the ICT department in line with business objectives. These standards may change periodically to keep up with technology changes. OCHL shall from time to time define the Company's standards relating to standard software with respect to: -

i) Operating System;

ii) Application Suite(s);

iii) Messaging Systems;

iv) Internet Access;

v) Data Base; and

vi) Database Programming

9. Hardware and Software Register

The ICT department will maintain a database of all the computer hardware and software owned by OCHL. Copies of this inventory will be forwarded to the Administration and Finance departments. The inventory will contain: -

i) Computer make and model (include monitor, keyboard, mouse, docking station, capacity);

ii) Processor type and speed;

iii) List of internal accessories and their rating (installed Expansion Slot Cards, Drives, etc.);

iv) List of external accessories and their ratings (printers, external drives, UPS, speakers, etc.);

v) Name of the current user and department;

vi) Asset ID tag number; and

vii) **Serial numbers of the above equipment should also be provided (where applicable).**

10. Hardware Maintenance and Repair

10.1.Maintenance

OCHL will maintain and purchase current industry-standard hardware equipment, wherever possible. The manufacturer of such equipment will provide a written warranty, which can be honored by the local vendors.

Maintenance contracts with reliable and economical external vendors will only be signed by ICT personnel. ICT will maintain contracts for special equipment (due to the scarcity of spare parts) such as the file servers, to limit downtime during breakdowns. **ICT should keep a log of all the hardware maintenance activities performed.**

10.2. Repairs

All faults should be reported and logged at the ICT Help Desk Central Support Office (CSO).

The computer's user should fill in the **Support Request Form (A7)** and forward it to the Help Desk for resource allocation and action. The users are advised to retain a copy of his/her support request for their records (the support request form can be obtained from the ICT public folder or from the Help Desk).

ICT, upon receipt of the request, will perform a diagnostic test to establish the cause of the problem and then update the support request form with the findings, before proceeding with the repairs. The following procedures will be adhered to for more complex repairs that cannot be managed internally:

i) The diagnostic report will be forwarded to the ICT Department Head for approval, who should first confirm the validity of the case.

ii) The ICT department will update the equipment user and his/her Department Head on the findings.

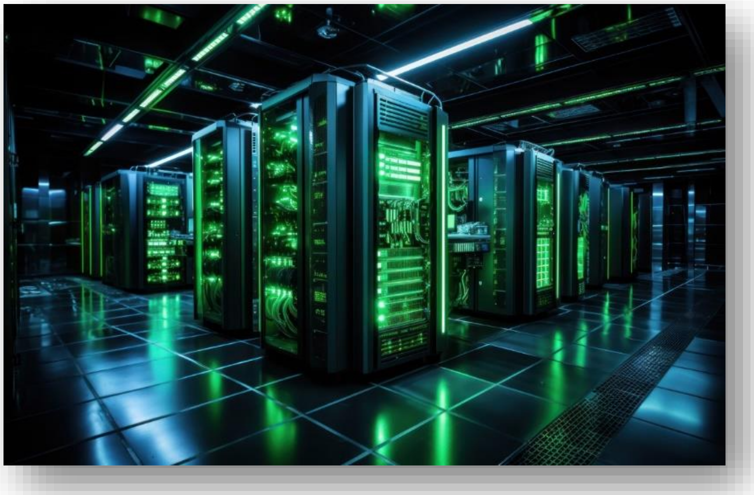
iii) ICT will contact the support vendor per the existing maintenance or warranty contract.

iv) There will be a need for a gate pass (**Equipment Gate Pass Form A2**) for any machine or accessory leaving OCHL for repair and a stamped Goods Received Note (GRN) from the vendor should be obtained. These forms will be filed by ICT in the Support Request File, alongside the support request form. Note that accessory and software details should be written on the Gate Pass.

v) A quotation or bill of material will be provided to the department head, once vendor diagnostics are available, for approval before the equipment is repaired; and

vi) After repair, the equipment will be returned to/received by the ICT Department Head or their designee to verify completion of work before returning it to the user together with the support request form for acknowledgment. ICT will retain a copy in the Support Request File for further reference.

11. Back-Up Operations and Procedures



Data is one of OCHL's most important assets. In order to protect this asset from loss or destruction, it is imperative that it be safely and securely captured, copied, and stored. The objective of this section is to outline a policy that governs how and when data residing on company servers will be backed up and stored for the purpose of providing restoration capability. In addition, it will address methods for requesting that backed-up data be restored to individual systems.

OCHL must ensure that the existing backup strategy and procedures are in line with state-of-the-art backup techniques. Further, the ICT department shall determine to what extent OCHL shall have a remote backup facility and prepare a recommendation for consideration by the GFD. The following backup and recovery strategies, policies, and procedures are based on these criteria:

11.1. Types of Back-ups

The following backup types are conducted at OCHL: -

i) **Copy backup** - A copy backup copies all the selected files but does not mark each file as having been backed up. Copying is useful in case there is a need to backup files between normal and incremental backup because copying does not affect these other backup operations.

ii) **Incremental backup** – This backs up files that have been created or changed since the last normal or incremental backup. It marks files as having been backed up. If you are performing a combination of normal and incremental back-ups, you will need to have the last normal as well as the last incremental back-up; and

iii) **Full backup** - This type of backup copies all files and folders and results in faster backup and restoration of operations.

11.2. Solution Design

OCHL shall, through the ICT department, develop the right hardware and software solutions that will achieve the backup solution that will meet OCHL's backup requirements.

11.3.What is to be backed up?

This policy refers to the backing-up of data that resides on OCHL's servers.

This policy does not encompass backing up of data that resides on individual PC or Laptop/Notebook hard drives. Responsibility for backing up data on local desktop systems or laptops rests with the individual users, who are strongly encouraged to save their data to the appropriate server listed above so that their data is backed up regularly per this policy. Tools are being developed for the desktop to assist users in this process, automatically picking for backup only those files that have changed since the last backup procedure. Regardless, such backup will still need to be initiated by the user.

It is the responsibility of the ICT department to ensure that all new computers and servers get added to the backup scheduling process and that this policy be applied to each new server's maintenance routine. Before deploying a new computer/server, a full backup must be performed, and the ability to perform a full restoration from that backup confirmed. Before retiring a computer/server, a full backup must be performed and placed in a data safe and remotely at a Data Centre.

11.4.Back-up Schedule

Full back-ups will be conducted automatically as scheduled (11:59 p.m.) on Mondays and Saturdays of every week. Server snapshots are also taken at an interval of thirty (30) minutes to OCHL local back-up Server and transferred to the offsite server immediately, as necessary. Should recovery be necessary these snapshots will reduce the rework that would otherwise be required. We have investigated the use of online real time back-up capabilities but none were available in Kenya.

The OCHL server back-ups will be done according to the following procedure. This will ensure that our back-ups can be quickly and efficiently resorted and that no more than one day's working data will be missing in the event of a data loss incident:

i. All backups shall be labeled using the following labeling conventions: (day, date, month, year);

ii. All backups stored on-site are to be stored in the fireproof safe located in the fire-protected Server Room.

iii. All backup data to be stored offsite shall be stored on the backup server located at a Data Centre approved by the Head of IT and the GFD prescribed according to this policy.

iv. All backups will take place between the hours of [11 p.m. and 1 a.m.]. This timeframe has been selected to minimize the impact of server downtime on end users that may be caused by the need to take servers offline to perform the backup itself. If this backup schedule in some way interferes with a critical work process, then the affected user(s) is to notify the ICT department so that exceptions or alternative arrangements can be made.

v. A full backup will be performed each day. The data will be stored on-site during the backup cycle. At the end of the latter cycle, the backup will be restored to our offsite server, and a similar copy stored at a Data Centre. At the end of the day, the full backup is transferred to the Data Centre and replicated to the other remote site.

vi. All manual full back-ups performed must be noted in the server backup log immediately upon completion. All server backup log sheets must be kept in an appropriately labeled fireproof safe and the label should include: -

a. **Server name,**

b. **Date and time of backup,**

c. **Name of administrator performing the backup,**

d. **Back-up name,**

e. **Software used to perform the backup,**

f. **Back-up medium used and its label/name, and**

g. **Whether the backup was successful or not.**

vii. If, for some reason, the backup cannot be completed, is missed or crashes, then it must be completed the following day. The reason for the non-completion of the originally scheduled backup must be noted in the server backup log. In addition, if a backup fails for more than one day, the GFD and Chief Executive Officer (CEO) must be notified.

viii. If a backup media is discovered to be damaged or corrupt, then the media must be destroyed to prevent further use and replaced with a new one. Back-up media will be recycled every six (6) months to prevent this occurrence.

11.5.Managing Restores

The ultimate goal of any backup process is to ensure that a restorable copy of the data exists. As a result, it is essential to regularly test one's ability to restore data from its storage media. This policy will require that:

i) All daily backup media must be tested at least weekly to ensure that the data they contain can be completely restored.

ii) All weekly backup media must be tested at least once every month to ensure that the data they contain can be completely restored.

iii) All monthly back-ups must be tested at least once every month to ensure that the data they contain can be completely restored and are reliable.

iv) Data will be restored from a backup if: -

a) There is an intrusion or attack which necessitates a restoration.
b) Files have been corrupted, deleted, or modified.
c) Information must be accessed that is located on an archived backup.

v) The individual responsible for overseeing backup and restore procedures is the ICT Department Head. If a user has a restore request, they can contact the ICT Department Head, sending an e-mail or filling out and submitting a request form (available under ICT resources on the Intranet).

vi) In the event of local data loss due to human error, the end user affected must contact the ICT Department and request a data restore. The end user must provide the following information: -

a) Name,
b) Contact information,
c) Name of file(s) and/or folder(s) affected (provide complete path),
d) Last known location of files(s) and/or folder(s) affected (provide complete path),
e) Extent and nature of data loss,
f) Events leading to data loss, including last modified date and time (if known), and
g) Urgency of restore.

vii) Depending on the extent of data loss, a daily back-up media, weekly back-up media or combination of both will need to be used. The timing in the cycle will dictate whether or not these media are on-site or offsite. Back-up media must be retrieved by the server administrator or pre-determined replacement. If backup media are offsite and there is a need for a restore then the end user affected may be required to wait up to one day for a time- and cost-effective opportunity for the media to be retrieved.

viii) If the data loss was due to user error or a lack of adherence to procedure, then the user responsible may be required to participate in a tutorial on effective data backup practices.

11.6.Recovery in the Event of a Loss of the Host Environment

This section intends to address the additional recovery steps that would be required if OCHL lost all or most of its system host systems to a disaster. It will address logistical issues of how people will communicate provisions for backup servers, migration strategies, and provisions for equipment. Inherent in this plan is the assumption that the company will have at least one viable backup from the remote backup sites described above. This section of the plan has not been finalized at this time but will be completed in conjunction with our Enterprise Risk Management (ERM) program assessment.

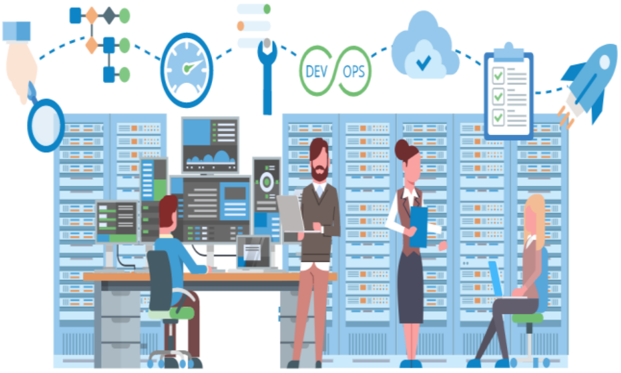
12. Training

Wherever possible, **Training within Industry (TWI) techniques** will be used to train users. To fully use the available technology, staff will need to develop appropriate levels of IT competencies. Every Department will need to assess the ICT skills of staff and encourage staff to attend training courses as appropriate. In order to meet developments in ICT and changing needs, the technical skills of ICT staff need to be developed in networking, business and systems analysis, web-based development, databases, and desktops through appropriate learning means.

13. System Infrastructure Change Management Policy

13.1.Purpose

The purpose of the System Infrastructure Change Management Policy is to manage changes to ICT Infrastructure rationally and predictably. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of our vital Information and Communication Technology infrastructure.



13.2. Policy Statement

A System Infrastructure Change Management Committee (SICMC) should be appointed by the CEO. These members meet as required to address infrastructure issues within the scope of this policy.

13.3. Scope

This policy covers **only major changes to hardware, software, or applications in the shared ICT infrastructure of OCHL.** This includes modification, changes, or additions to our network services (LAN/WAN), server hardware and software, and the ICT environment (such as electricity). Any change that might adversely affect the ICT infrastructure is within the scope of this policy.

Changes to the ICT Infrastructure may be necessary for many reasons, ranging from the need to fix a hardware problem to the need to update software. Here is a non-exhaustive list of change sources:

- **i) Periodic maintenance.**
- **ii) User requests.**
- **iii) Hardware and/or software upgrades.**
- **iv) Acquisition of new hardware and/or software.**
- **v) Other changes or modifications to the infrastructure.**
- **vi) Environmental changes; and**
- **vii) Operations schedule changes.**

13.4. System Infrastructure Change Management Committee (SICMC)

The SICMC will receive all requests for changes. Requests for changes must be made through the **Change Request Form**. The Change Management Committee will have the following terms of reference:

i) To meet as necessary to review all requests for change with the requestors on time.

ii) To be responsible for mapping out the potential impact of the change on stakeholders.

iii) To be responsible for communicating to all stakeholders such critical information about how a change will/could impact their work.

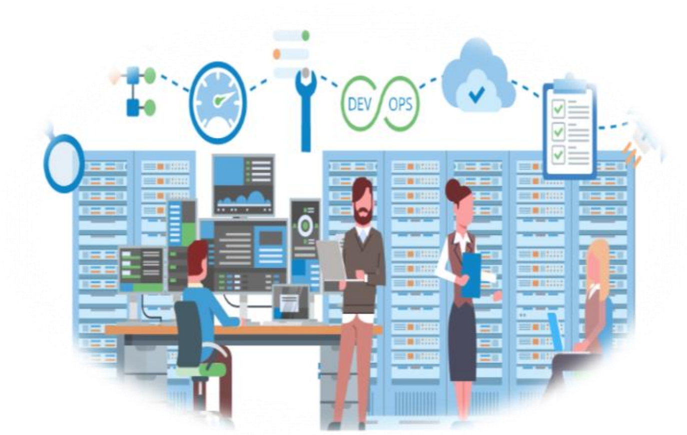
iv) To assess the urgency and potential impact of proposed changes. High-impact changes, for example, might require downtime outside of regular maintenance cycles.

v) To ensure that changes to critical hardware and software systems meet testing and approval criteria in advance of making the change; and

vi) To be responsible for documenting and accounting for all changes. The SICMC will maintain a change log that documents all requests for change, plans and scheduling of the change, and track outcomes.

13.5. ICT Infrastructure Change Management Procedure

The change management process shall include the following steps. Each of these steps must be completed for every change:



i) The requestor fills out a change management form. The form includes space for a detailed description of the proposed change, the systems involved, the business units impacted, and the location impacted. The requestor also makes an initial assessment of the urgency and potential risk of the change with the help of the ICT Department Head, how much implementing the change will cost, and how much downtime the change may require.

ii) The SICM Committee reviews and approves the change. At its regular meeting, the Committee will review the Request for Change. The group will evaluate the requestor’s proposal in light of their knowledge of OCHL technologies, business processes, and interdependencies.

iii) The SICM Committee can send the request back to the requestor for further detail and study if needed.

iv) The SICM Committee assigns responsibility for making the change. If the request is approved, the Committee will assign responsibility for making the change to ICT personnel. They will establish specifications and testing requirements depending on the nature of the change, based on the recommendation of the SICMC.

v) The SICM Committee will communicate with stakeholders. The Committee will make sure that all stakeholders are aware of the nature and potential impact of the proposed change. For changes requiring downtime outside of regular maintenance cycles, the group will also request feedback from stakeholders on the most appropriate timing of downtime.

vi) The SICM Committee will track progress on the proposed changes. Personnel assigned to implement such changes will report back to the Committee regarding progress. When the proposed change has been tested, and the appropriate fallback plan is in place, the change shall be formally scheduled and communicated to the stakeholders and

vii) The SICM Committee will perform a post-mortem review of all changes. At their regular change management meetings, the SICM Committee shall perform post-reviews on all changes. Successful changes and lessons learned from the experience will be documented in the change log by the ICT Team.

13.6. Emergency Changes

Any critical, non-standard operational event, such as a system failure that has or could pose a significant service delivery interruption, is coded as the *highest severity* incident for prioritizing, monitoring, escalation, resolution, and archiving. These are events that have been detected either from monitoring of the network, event log monitoring by in-house staff, or by detection on the part of any employee and/or user.

The ICT department staff monitors the server, network environment, and log system daily for non-standard events. This occurs through several processes:

i) Internal event log monitoring,

ii) External monitoring,

iii) User reporting through the Help Desk function.

iv) Emergency events are logged once identified, either by regular ICT monitoring or through user requests; and

v) After being identified and logged in the log system, all priority events are escalated to the ICT Department Head and a notification is sent via email. Distribution is to the GFD with copies to the executive management team.

14. ICT Asset Disposal Policy

The purpose of this Section is to establish and define standards and procedures for the disposal of non-leased ICT equipment in a legal, cost-effective manner. OCHL surplus or obsolete ICT assets and resources (i.e., computers, servers, databases, etc.) must be discarded according to legal requirements and environmental regulations through the appropriate external agents. Therefore, all disposal procedures for retired ICT assets must adhere to company-approved methods.

This policy applies to the proper disposal of **all non-leased OCHL's ICT hardware**, including PCs, printers, handheld devices, servers, databases, hubs, switches, bridges, routers, and so on. **Company-owned surplus hardware, obsolete machines, and any equipment beyond reasonable repair or reuse are covered by this policy**. Where possible it is desirable to achieve some residual value of the IT asset in question through reselling, auctioning, donation, or reassignment to a less-critical function.

14.1. Guidelines

Disposal and disposal procedures of all ICT assets and equipment will be centrally managed and coordinated by OCHL's ICT department. OCHL's ICT department is also responsible for backing up and then wiping clean company data, all ICT assets slated for disposal, as well as the removal of company tags and/or identifying labels. The ICT department is in charge of selecting and approving external agents for recycling hardware and/or sanitizing hardware of harmful toxins before shipment to landfills.

14.2. Policy

It is the responsibility of any employee within OCHL's ICT department, with the appropriate authority, to ensure that ICT assets, equipment, and hardware are disposed of according to one or more of the methods prescribed above. Any disposals performed by OCHL must be done appropriately, responsibly, and ethically, as well as with company resource planning in mind. The following rules must therefore be observed:

i) **Obsolete IT Assets:** Identifying and classifying ICT assets as obsolete is the sole province of OCHL's ICT department. Decisions on this matter will be made according to OCHL's purchasing/procurement strategies. Equipment lifecycles are to be determined by ICT asset management best practices (i.e., total cost of ownership, required upgrades, etc.).

ii) **Reassignment of Retired Assets:** Reassignment of computer hardware to a less critical role is made at the sole discretion of the Company's ICT department. It is the goal of OCHL, whenever possible, to reassign ICT assets in order to achieve the full return on investment (ROI) from the equipment and to potentially minimize hardware expenditures by reassigning hardware to another business function.

iii) **Trade-Ins:** In cases in which a piece of equipment is due for replacement, reasonable actions must be taken to ensure that a fair and market trade-in value is obtained for the old ICT asset against the cost of the replacement. OCHL's Procurement Manager or ICT Manager will assume this responsibility.

14.3. Income Derived from Disposal

Whenever possible, it is desirable to obtain some residual value from retired or surplus ICT assets. Income derived from sales to staff, the public, or through online auctioning must be fully received and monies sent to OCHL's Finance department. Sales to staff should be advertised through the company intranet or via e-mail. The CEO and GFD should approve all sales below fair market value.

14.4. Cannibalization and Assets beyond Reasonable Repair

The ICT Manager is responsible for verifying and classifying any ICT assets beyond reasonable repair. Such equipment should be cannibalized for spare and/or working parts that can still be put to use within the organization. The ICT department will inventory and stockpile these parts. The remaining parts and/or whole machines unfit for use or any other disposal means will be sold to an approved scrap dealer or salvaging company.

14.5. Decommissioning of Assets

All hardware slated for disposal by any **means must be wiped clean of all company data**. OCHL's ICT department will assume responsibility for decommissioning this equipment. This sanitizer must completely overwrite each and every disk sector of the machine with zero-filled blocks. In addition, any property tags or identifying labels must also be removed from the retired equipment.

14.6. Harmful Substances

Hazardous materials such as lead, mercury, bromine, cadmium, etc. must be thoroughly removed from computer hardware before shipment to a landfill as rubbish. The ICT department may perform this action itself using government-approved disposal methods or hire an accredited disposal company specializing in this service. No matter the route taken, the removal and discarding of toxins from OCHL ICT equipment must be in full compliance with local and federal laws.

14.7. Donations

ICT assets with a net residual value of less than Kenya Shillings Five Thousand (KES 5,000/-) that are not assigned for reuse, discarding, or sale to employees or external buyers may be donated to a company-approved school, charity, or other non-profit organization (i.e., a distributor of free machines to developing nations). All donations must be authorized by the CEO. **All donation documentation must be submitted to the Finance department for taxation purposes.**

14.8. Notification of Accounting

Forms required by the "Capital Assets Disposal Policy" should be complete and submitted upon disposal of the ICT assets. In this case, this form should be accompanied by an email from an authorized individual that this asset was disposed of per this policy.

15. ICT Security Register

OCHL shall put in place an **ICT Risk Register** to document breakdowns in any ICT functional areas. At a minimum, the register shall contain the following details:

i) **Affected area,**

ii) **Description of the incident,**

iii) **Control in place and why they failed,**

iv) **Action summary,**

v) **Action deadline,**

vi) **Responsibility,**

vii) **Consequences,**

viii) **Likelihood of reoccurrence,**

ix) **Rating,**

x) **Function, and**

xi) **Other references**

16. Security Access Matrix for ICT Systems

OCHL shall develop a security access matrix for all users of the Company's system. At a minimum, the access matrix should show:

i) **User ability to access modules within the ICT system.**

ii) **User ability to add/edit/delete records within a module.**

iii) **Users access within the ERP system to multiple roles**

iv) **Segregation of duties issues within systems**

17. Amendments

Changes to this policy will be approved and amended by the Board from time to time and communicated to staff.

18. Effective Date

This policy is effective immediately.

Last update and review: March 7, 2024

19. APPENDICES

OLYMPIA
Capital

A1 - Change Management Form

1. Describe the proposed change.

____

____

____

____

2. Identify the Systems involved or impacted.

____

____

____

____

3. State the business units affected.

____

____

____

____

4. The assessment of the level of risks to other company systems done in conjunction with the IT Team Lead. (High, Medium, Low)

____

____

5. State the urgency of the change (High, Medium, Low) and the reasons for this assessment.

6. State the cost of implementing the changes (in KES). This will be done in consultation with the IT Team Lead.

7. Estimate the time required for the change (Hours). This will be done by IT Team Leader.

8. Change categorization (Large, Medium, small).

9. The deadline for the change (1 day, 2 days, 1 week, 2 weeks, 1 month).

____

____

____

____

10. Back-out plans – *For official use* (To be developed by the IT Team Lead).

____

____

____

____

11. User acceptance (State whether the required change is met).

____

____

____

____

12. Evidence of user acceptance testing ***(User sign off)***

____

____

____

____

13. Escalation procedures ***(for official use)***

____

____

____

____

14. Review and closure of changes ***(for official use)***

____

____

____

15. Types of changes ***(Planned, Emergency)***.

____

____

____

____

16. Change Approved /Rejected

Signature: ______________________

Date: ______________________

Title: ______________________

Other comments

____

____

____

____

A2 - IT Department Gate Pass

Date: _______________

This is to certify that the person/s named below has permission to carry the listed items out of the building for service.

Name: ____

Company: ____

Quantity	Item Description	Serial number, if applicable

Additional Comments:

____

____

____

Thank you.

I.T Team Lead

Signature: ____________________________

Contact Number: ____________________________

Date: ____________________________

A3 - Access Application Form General Information

Date of request: ____________________________

Date access is required: ____________________________

User's Full Name: ____________________________

User Contact Number: ____________________________

User Designation: ____________________________

User Staff Number: ____________________________

User Branch: ____________________________

User Department: ____________________________

Previous user in this role: ____________________________

Comment on responsibility difference (new vs. predecessor):

____

____

____

____

Specific Request

Please grant/change/revoke the above-named person access to the following ERP Modules/sessions. (Delete as appropriate) or indicate the established role (s).

____

____

____

____

Companies to which access should be given: ____

Warehouse accesses: ______________________________________

List any date or other restriction on these accesses:

____

____

Head of Department: ____________________

Signature: ____________________

Date: ____________________

Finance Sign off

I have reviewed the aforementioned access changes for potential segregation of duties and other control issued and believe there are none (any concerns should be brought to the GFD's attention)

Chief Accountant: ____________________

Signature: ____________________

Date: ____________________

I.T. Sign Off

Change Approved by: ______________ Signature: ____________________Date: ____________

Change Verified by: ______________ Signature: ____________________Date: ____________

Change Effected by: ______________ Signature: ____________________Date: ____________

Account valid until: ______________________________

I ______________________________ understand that I am the only person authorized to use my login name, password, and granted permissions. I take full responsibility for the use, misuse, and execution of my login name, password, and permissions. I further agree not to copy or share this information with anyone not called out in my job description without express written permission of the CEO.

User Signature: ________________________ Date: ______________________________

Note: These permissions supersede any other earlier granted permission.

A4 - Equipment Movement Form

Equipment type (CPU, Monitor, Keyboard, Mouse, Scanner, Printer, Fax, copier, Router, Microwave radio, Laptop) or other specify ***(Tick as appropriate)***

Date of Request: ______________________________

Date of Move: ______________________________

Requestor: ______________________________

Designation: ______________________________

Equipment Asset Number: ______________________________

Serial number(s): ______________________________

Current user: ______________________________

Users contact number: ______________________________

Current location of the equipment: ______________________________

Department: ______________________________

Reason for movement: (Repair, Disposal, Transfer) other specify:

____

____

____

Destination location: ______________________________

Department: ______________________________

New User: ______________________________

Contact Number: ______________________________

Requestor Signature: ______________________________

Date: ______________________________

Receiving Section

I ______________________________ have received the aforementioned equipment in (Good, faulty) condition.

Description of faults (if any):

____

____

____

____

Signature: __________________________________

Date: __________________________________

Finance sign-off (as required)

I _____________________ have transferred the equipment in the books and records of the related companies.

Signed: __________________________________

Date: __________________________________

Department/Section Stamp

To be filled in triplicate and copy retained for follow-up. Receiving section to stamp and return to sending site for confirmation of receipt.

A5 - Request for Training

Username: ______________________________

Contact Number: ______________________________

User's Location: ______________________________

Department: ______________________________

Previous Role(s): ______________________________

Current Role (s): ______________________________

State the training need:

____

____

____

____

I request that this aforementioned training be undertaken.

Requestor: ______________________________

Signature: ______________________________

Date: ______________________________

Department/Section

Tick as appropriate

o This training can be adequately covered by our department/section, or
o This training cannot be adequately covered by our department/section.

Trainer's Comment

______________________ can effectively perform his/her current role in with respect to the aforementioned training.

Name: ________________________________

Signature: ________________________________

Date: ________________________________

Trainee's Comments

I _________________ can now effectively function in the role of ______________without supervision.

Name: ________________________________

Signature: ________________________________

Date: ________________________________

A6 - E-Mail and Internet Connection Request Form

Date of request: ______________________________

Date access is required: ______________________________

User's Full Name: ______________________________

User Contact Number: ______________________________

User Designation: ______________________________

User Branch: ______________________________

User Department: ______________________________

Is Internet access required in the job: Y/N

Please indicate that this account needs to remain active, If this is a temporary position:

From __________________________________ to ____________________

Please indicate Distribution Lists the employee should belong e.g., Head Office All

1. ____
2. ____
3. ____
4. ____

Has the User read and signed the Internet Email and Browsing Policy Y/N
(attach an executed copy)

User Department Head: ______________________________

Dept. Heads Contact Number: ______________________________

Other Comments:

____

____

____

____

Dept. Head Approval: ______________________________

Date: ______________________________

I.T. Leads Approval: ______________________________

Date: ______________________________

OLYMPIA
Capital

A7 - Support Provision Form (completed by I.T.)

Problem report Details

Name of customer: ______________________________

Contact number(s): ______________________________

Department: ______________________________

Workstation location: ______________________________

Date: ______________________________

Time: ______________________________

Equipment Make and Model: ______________________________

Serial number: ______________________________

Service tag Number (on back or bottom): ______________________________

Accessories impacted:

____

____

Specific Problem Statement:

____

____

____

____

Solution_Provided

____

____

____

Was problem resolved Y/N (tick as necessary) What follow up, if any, is required: ____

____

____

Is the requester satisfied with the solution Y/N (tick as necessary) If no, why: ____

____

____

____

User's signature: ____________________________

I.T person Signature: ____________________________

For official use only

IT Staff Name: ____________________________

Time spent: ____________________________

IT Leads comments/observations: ____

____

Signature: ____________________________

Date: _________________________

A8 - Purchase Authorization Form

Request By: ______________________________

Date: ______________________________

Department: ______________________________

Designation: ______________________________

Description of Equipment / Software required:

____

____

____

Estimated cost: ______________________________

Was this item in the budget; Y/N (please tick one) If in the Budget, the amount budgeted:

____

____

All equipment purchases need to go through procurement.

Reasons for Purchase:

____

____

____

Alternative considered:

____

____

____

____

Replacing Old Software / Equipment? Y/N

Details of Old Equipment including asset tag number and serial number:

____

____

____

Approvals

Purchase Requisition approved by: ________________________________
(Department Head)

Designation: ________________________________

Date: ________________________________

I.T Comments:

____

____

____

____

A9 - Equipment Authorization Form

User/Supervisor Information

User’s Full Name: ______________________________

Users Designation: ______________________________

User’s Branch: ______________________________

Users Department: ______________________________

User’s Dept Head: ______________________________

Dept. Head Approval: ______________________________

Date: ______________________________

Equipment Information

Equipment Make: ______________________________

Equipment Model: ______________________________

Condition of Equipment:

____

____

____

Asset Tag Number: ______________________________

Serial Number: ______________________________

Accessories provided with Equipment:

____

____

____

Comments on condition of accessories:

____

____

____

____

User Acknowledgements

I the undersigned acknowledge receipt of the aforementioned asset(s) and understand that I am fully responsible for these assets in event of loss, theft or damage.

User Signature: ______________________________

Date: ______________________________

I.T. Department Details upon deployment

I.T. Person servicing request: ______________________________

Designation: ______________________________

Comments and observations:

____

____

____

____

Signature I.T. Rep: ______________________________

Date: ______________________________

Equipment Returns/Lost Information

Date of Return: ______________________________

Missing Items:

____

____

Means of repayment, if applicable:

____

____

____

Other I.T. Observations:

____

____

____

____

Signature of User: ______________________________

Date: ______________________________

Signature of IT Rep: ______________________________

Date: ______________________________

Other Comments:

____

____

____

A10 - Network user Creation/Amendment Form

User Surname: ______________________________

Other Names: ______________________________

Department: ______________________________

Grant the above users access to the network for the period

Starting: /____ / (if known)

To: /____ / (if known)

User Account Attributes;

Email Account (Yes/No)
Internet Access (Yes/No)
Public Folder Access (Yes/No)

Please specify any other systems/applications/network resources that the user should have access to:

____

____

Please provide the predefined roles that apply to this individual:

____

____

IT Comments:

____

____

Requested Authorized By: ______________________________
(Departmental Head)

Finance approval: ______________________________

A/C Created By: ______________________________
(IT Officer)

This form should be filled in triplicate (1) IT (2) Departmental Head (3). Administration

A11 - Internet Email and Browsing - User Acknowledgements

I acknowledge and understand that to keep OCHL computers running effectively and efficiently, and to ensure that maximum network capacity is available for everyone to do their work, the following general policies regarding the security and operation of the OCHL computer network apply:

1. Use of OCHL network and information resources for non-business purposes should be kept to a minimum. Limit personal e-mail and Internet traffic, particularly during regular working hours. Such rights can be withdrawn at the discretion of management if one is suspected of misuse.
2. Any employee who illegally secures Internet access without approval will dismissed.
3. Downloading software from the Internet that is not licensed to OCHL, verified, approved, or supported by OCHL is prohibited.
4. Use caution in opening e-mails from unknown sources. Immediately delete suspicious messages, leaving the attachment unopened. Immediately notify the ICT department. Even though your computer is protected by anti-virus software, the threat of a virus attack still exists.
5. Non-business-related high-volume traffic over the network that hinders colleagues in their use of business applications is prohibited. Examples include:
   i) Internet radio station or similar accesses
   ii) Software downloads
   iii) Audio and Video downloads or real-time streaming media
   iv) Excessive personal email attachments and downloads
   v) Distribution of hoaxes, chain letters, or advertisements over the network.
6. Users, with permission, accessing the network, email, or the Internet, using their equipment, will be required to have up-to-date and OCHL-approved anti-virus protection.
7. Any user who requires an e-mail account or Internet access must seek written authorization from his/her respective Department Head. ICT will then use a process to allocate and maintain e-mail accounts and Internet access. Each user will have a unique username and password as described above.

I have read and acknowledge that I agree to comply with the aforementioned policy. I further understand that should I fail to comply I could lose my access to the internet and email and could be subject to dismissal.

Username: ______________________________

Title: ______________________________

Date: ______________________________