Uganda Electricity Transmission Company Limited

ICT Policies and Procedures Manual

December 2022

Version	Date Completed	Steer Com Approval	Mgt. Approval Date	BoD Approval Date
4.0	**10th April 2021**		**27th September 2021**	**3rd November 2022**

1 Table of Contents

1 List of Acronyms

CBP	- Corporate Business Plan
CCTV	- Closed Circuit Television
CEO	- Chief Executive Officer
CERT-UG	- Uganda National Computer Emergency Response Team
CSD	- Corporate Services Department
CUG	- Closed User Group
DCEO	- Deputy Chief Executive Officer
DLP	- Data Loss Prevention
DRM	- Digital Rights Management
ERA	- Elec….. Reg………..Authority
FAS	- Finance, Accounts and Sales
FASD	- Finance, Accounts and Sales Department
FOA	- Fiber Optic Association
HRA	- Human Resource and Administration
HRAD	- Human Resources and Administration Department
IAD	- Internal Audit Department
ICT	- Information and Communication Technology
ICTSP	- ICT Strategic Plan
IR	- Infrared
IS	- Information Systems
IT	- Information Technology
ITIL	- Information Technology Infrastructure Library
KPI	- Key Performance Indicator

LAN	- Local Area Network
MD	- Managing Director
MHRA	- Manager Human Resources and Administration
MICT	- Manager Information and Communication Technology
MIS	- Management Information System
MoICT	- Ministry of Information and Communications Technology
NITA-U	- National Information Technology Authority of Uganda
NISF -	National Information Security Framework
NITP	- National IT policy
OEM	- Original Equipment Manufacturer
OFI	- Optic Fiber Infrastructure
OIC	- Online Information Committee
OMD	- Operations and Maintenance Department
PCs	- Personal Computers
PCE	- Principal Communication Engineer
PDA	- Personal Digital Assistant
PID	- Project Implementation Department
PIN	- Personal Identification Number
PITO	- Principal Information Technology Officer
P&ID	- Planning and Investment Department
PLC	- Power Line Carrier
PPDA	- Public Procurement and Disposal of Public Assets Authority
RDBMS	- Relational Database Management Systems
SCADA	- Supervisory Control And Data Acquisition System
SMAT	- Specific, Measurable, Achievable and Time bound

SSA	- Software Support Agreement
SSLA	- Software Service Level Agreement
UETCL	- Uganda Electricity Transmission Company Limited
UCC	- Uganda Communications Commission
USB	- Universal Serial Bus
VoIP	- Voice over Internet Protocol
VPN	- Virtual Private Network
WAN	- Wide Area Network
WiFi	- Wireless networking Technology using radio waves to provide wireless high-speed internet and network connections.
ITU-T G	- International Telecommunication Union standard for a Transmission System, Media digital system and Networks.

2 List of Definitions

Access Codes: An alphanumeric sequence that permits access to an ICT device or network.

Authentication: Validating UserID and password or access code.

***Authorized User*:** Also called *User.* A person granted rights to use a specific ICT system or resource.

***Backup*:** To create a copy of critical files to minimize loss of data in the event of a system failure.

Business continuity: Is the activity performed by the ICT department to ensure that critical business functions will be available to UETCL internal and external customers.

Change: Equipment rearrangement or configuration updates

Computers: Electronic devices designed to accept data, perform prescribed mathematical and logical operations at high speed, and display the results of these operations.

Corporate: Shall mean UETCL

Corporate Internet: Internet services provided by UETCL to staff through UETCL's centralized Computer Local Area Network.

Critical Business Data: Users' operational files kept on the shared folders, emails or data generated by mission critical business applications such as SUN, SCADA etc.

Corporate Phones: Desk phones and Business Closed User Group (BCUG) mobile phones.

Designated user: Authorized user who has been assigned an ICT equipment for use in his/her day-today tasks.

Electronic Resource: Material in digital format which requires an electronic device to access

Email: A short name for 'Electronic mail'. It is the means or system for transmitting messages electronically between computers on a network. Also used to mean *a* message sent and received electronically through an e-mail system.

ERA: Electricity Regulatory Authority

Firewall: A system access control device that acts as a barrier between two or more segments of a computer network to protect internal networks from unauthorized users or processes of other networks.

Encryption: A data security method used to transform data from its original form into a coded format which is difficult to interpret in order to prevent any unauthorized recipient from reading it.

ICT Department: The UETCL department responsible for the management and support of all computers, networks and communication systems.

ICT Infrastructure: All ICT hardware and software systems.

ICT Systems: This is used to mean ICT Hardware, Software, Data or Information. Examples are; Computers, Servers, Printers, Networks, Storage media, Photocopiers, Software, Unified VoIP Communications systems, Mobile phones, Battery banks, Battery chargers, Generators, Fax machines, Power backups, Optic fiber infrastructure, Wireless equipment, Power line carries, Optical Domain Frames, fiber multiplexers, Racks, Media converters, Email, Internet and any other ICT equipment used in UETCL. Power system control, dispatch and the underlying infrastructure.

Information resources: The data and information assets of UETCL located on UETCL's ICT systems.

Internet: An electronic communications network that connects computer networks and organizational computer facilities around the world to facilitate sharing of global information.

Intranet: A computer network that uses Internet Protocol technology to share information or computing services within an organization.

Logon: *see "Username"*

MO&M: ***Manager Operations and Maintenance***

Mobile Computing: Using technology in a non-fixed location via a portable computing or communication device such as a laptop, tablet or cell phone.

Operational Phone: A corporate post-paid mobile phone used by staff for operational work.

Password: A string of private characters that grants user access to an ICT system.

Personal Files: Any type of electronic record, information or data file belonging to an individual and does not in any way relate to the UETCL or UETCL business.

Pirated Software: Unlicensed software.

PITO: Principal IT Officer

Policy Approver: The ICT Steering Committee and UETCL Board of Directors.

Policy Owner: A UETCL employee directly in charge of enforcing a given ICT policy.

Privileged Information: Information whose access is exclusively confined to a specific user or group of users.

Pr. Com Eng: Principal Communication Engineer

Pr. Ctrl Eng. Principal Control Engineer

Reasonable Efforts: Efforts based on known statements, events, or conditions. Reasonable efforts are defined as being within common sense, known best practices, or logical actions.

Remote Access: The ability to obtain right of use to UETCL ICT system from a location or via a system not owned by UETCL.

Residential Internet: Mobile internet installed on UETCL staff home Computer, Laptop or operational mobile phone for staff. It includes data services such as WiMAX, 3G and Blackberry on mobile phones.

Security: Measures taken to ensure a reliable ICT infrastructure which is free from any risk.

Server**:** A computer or computer program that manages access to a centralized resource or service in a network.

Software: The programs, routines and symbolic languages that control the functioning of the ICT hardware and direct its operation.

Spam: Unsolicited mass electronic mailings.

System Administrator: An ICT system user with privileges to alter systems settings.

TCP/IP: 'Transmission Control Protocol/Internet Protocol'. It is a combined set of communication protocols used to perform data transfers between computers over the Internet.

Tele-presence: Refers to a set of technologies which allow a user to feel and give appearance of presence as if they were present at a place other than their true location.

UserID: *see "Username".*

Username: Also referred to as "userID". A unique string of characters used to identify an ICT system user.

Virus: A dangerous piece of programming-code that attacks computer and network systems with the aim of causing them to malfunction. This includes; spyware and malware.

Webmaster: Person responsible for designing, maintaining and updating the website.

Wireless Network: A network utilizing radio waves to transmit data as opposed to physical wired connections. Example of a wireless network is Wi-Fi.

3 Introduction

UETCL previous version of this document (approved in 2017) was focused on ICT policies and guidelines applicable to the available resources and their usage. This version has been designed to close the gaps in the previous versions and incorporate emerging technologies. The major and significant new developments include the introduction of ICT procedures and the incorporation of internal service level agreements. Auditor's concerns picked from audit reports of subsequent years have also been incorporated. The policies and procedures in this document have been designed to carefully control the growth and operation of the ICT function and its cost, consistent with UETCL's goals and objectives as set in the Corporate Business Plan (CBP). These policies and guidelines apply to usage of all UETCL's ICT Systems and equipment as defined. It is therefore imperative that they are clearly read, understood, implemented and complied to by all users of UETCL's ICT facilities in a manner that will result into efficient and cost-effective operation of the ICT facilities.

4 Background

Uganda Electricity Transmission Company Limited ("UETCL", "the Company") is a Public Limited Company which was incorporated on 26th March 2001. The Company operates under policy guidance of the MEMD and is regulated by the ERA. The ICT function is further regulated by NITA-U and UCC.

UETCL is one of the three successor companies created as a result of the unbundling of Uganda Electricity Board ("UEB"). It is a public limited liability Company owned by the Minister of Finance, Planning and Economic Development and the Minister of Finance in charge of Privatization.

The Company holds four licenses issued by the Electricity Regulatory Authority:

i. System Operator;
ii. Operation and Maintenance of the High Voltage Transmission Grid;
iii. Power Import and Export;
iv. Bulk Power Supply.

The Company also has a license from Uganda Communication Commission as a public infrastructure provider authorizing the commercialization of the excess optic fiber and capacity on the UETCL power grid.

UETCL's operational mandate is to play two key functions:

i. **Transmission system operator:** system operations and maintenance of the high voltage electricity transmission network (above 33kV).

ii. **Single buyer:** bulk purchase and sale for all grid-connected electricity, including import and export of electricity.

4.1 Vision

UETCL's vision is;

"Electricity Transmission for Sustainable Regional Development ".

4.2 Mission

UETCL's mission is;

"To Buy, Transmit and Sell Quality Bulk Power".

4.3 Objectives of the Policies and the Procedures Manual

Ensure compliance with statutes, regulations and industrial standards concerning ICT in general.

To ensure consistency and reduce variation within a given process leading to a systematic way of executing tasks in the ICT department.

- Gain employee cooperation, compliance, and instil in the employees a sense of direction.
- To bridge the skills gaps for new ICT staff and to those changing job positions.
- Introduce business process documentation, checklists, workflows, rules and standards within the ICT operations.
- Transform the ICT department business philosophy, objectives, and goals into results-oriented actions.
- Introduce a valuable communication mechanism for efficiently driving the departments operations.
- Facilitate timely and informed decision making.
- Ensure optimum business operations and consistent delivery of ICT services to other departments within UETCL.

4.4 Legal Framework

The manual shall be guided by and interpreted in accordance with the following ICT frameworks, National laws and policies: -

- The Electronic Signatures Act, No.7, 2011
- The Computer Misuse Act, No.2, 2011
- The Uganda Communications Act, CAP 106
- The Access to Information Act, No.6, 2005
- The Copyright and Neighboring Rights Act, No.19, 2006
- The Data Protection and Privacy Act, 2015.
- The Electronic Media Act, CAP 104
- The Electronic Transaction Act, No.8, 2011
- The National IT Policy of MoICT (2010).
- The Telecommunications Policy of MoICT, 1996

- Information Services Management Policy of MoICT, 2012
- UETCL Staff regulations, November 2008
- UETCL’s Online Information Committee Terms of Reference, 2012
- Information Technology Infrastructure Library (ITIL)
- UETCL Communication policy, 2017
- National Information Technology Authority - Uganda (NITA-U) Act, 2009
- NITA-U Guidelines and standards for acquisition of ICT hardware and software for government ministries, departments and agencies, March 2013.

4.5 Reviews to the manual

There shall be an ICT steering committee appointed by the Managing Director/CEO, which shall, in addition to other duties, be responsible for formulation and/or review of ICT policies and procedures. The committee shall comprise of Manager ICT as the Chairman and a representative from each of the departments.

On an annual basis, the committee shall assess the need for a complete update to the Manual. When this need is identified, the Manager ICT shall initiate the process for updating the Manual.

4.6 Compliance Responsibility

The MD/CEO as the Accounting Officer of UETCL is ultimately responsible to the BoD for ensuring compliance with this Manual.

The Manager ICT shall be responsible for implementation of the ICT policies and procedures manual. All users of UETCL ICT systems and services shall be required to read, understand and comply with this manual through undertakings on ICT form 10. The Policy owners shall closely monitor and enforce compliance.

This Manual shall remain in draft form until approved by the BoD.

Other Manuals which interface this Manual are:

i. Staff Rules and Regulations;
ii. Financial Policy and Procedures;
iii. Internal Audit Manual;
iv. Insurance Policy; and

5 The ICT Department

The responsibility of the Information and Communication Technology Department lies within the Efficient Business Processes and Financial Sustainability focus area. Specifically, ICT enables UETCL achieve its corporate objectives in a cost-effective manner by:

- Offering reliable ICT support services to UETCL critical business processes.
- Providing timely and efficient ICT based support to employees.
- Enforce ICT security for UETCL data and systems.
- Aligning ICT strategy and plans with the overall corporate business strategy and plans.
- Evaluation and mapping of future user ICT needs within UETCL through Forecasting, Planning and carrying out ICT investments.
- Maintaining efficient ICT infrastructure in UETCL through carrying out preventive and corrective maintenance to the infrastructure.
- Marketing and leasing optic fiber infrastructure and the associated services.

The department has got two sections; Communication section and IT section.

5.1 Communication Section

The services offered by the communication section shall include;

- **Communication links;**
  - Design, Installation and Maintenance of communication links in support of;
    - SCADA
    - IT
    - Tele-Metering
    - Tele-Protection
- **Auxiliary power supplies including;**
  - Design, Installation, Maintenance and support of;
    - 48Vdc power supplies for telecom, control and IT devices in substations
    - 110Vdc for powering protection systems
    - Standby generators
- **Telephony services including;**
  - Design, Installation, Maintenance and support of VoIP services
  - Maintenance and support of Closed User Group (CUG)
  - Maintenance and support of satellite television and related services
  - Maintenance and support of Ordinary Land lines and Fax
- **Fiber infrastructure management**
  - Design, Installation, Maintenance, Marketing and leasing optic fiber infrastructure and the associated services.
- **Substation and Buildings Automation Systems**
  - Maintenance and support of building management systems
  - Maintenance and support of substation automation systems

5.2 IT Section

The services offered by the IT section shall include;

5.2.1 IT Infrastructure Maintenance and Support

i. Staff hardware facilitation
ii. Routine and corrective hardware maintenance
iii. IT Network maintenance (repairs and extension)
iv. SAN Data Storage Management
v. Virtualization Platform maintenance
vi. Accessories management (Print cartridge, CD/DVD, pen drives, etc.)
vii. Clean power (UPS power) installation, maintenance and support
viii. CCTV surveillance installation, maintenance and support
ix. IT/OT and smart grid interfacing technologies
x. Access control and time & attendance
xi. Maintenance and support of building management systems

5.2.2 IT Systems Administration and Support

- Critical Business Applications maintenance and support
    - Sun Systems
    - HR/Payroll
    - UETCL-Connect,
    - BIS
    - WIS
    - GIS
    - ERP
- Operating the IT Help Desk
- Database administration (Oracle, MSSQL, MySQL)
- Systems analysis, design and development
- IT security management (Firewalls, Cisco ISE and Antivirus)
- Internet and email Services provision (Fixed and Roaming)
- Intranet and website maintenance
- Access Control and time and attendance system support
- Systems backup and recovery

6 Steering Committee

6.1 Policy

i. There shall be an ICT steering committee appointed by the Managing Director/CEO, which shall, in addition to other duties, be responsible for formulation and/or review of ICT policies and procedures. The committee shall comprise representatives from each of the departments.

ii. The Principal IT Officer, Principal Communication Engineer and Principal Control Engineer shall constitute the secretariat of the Steering Committee.

6.2 IT Steering Committee Roles

The primary roles of the ICT Steering Committee shall be to:

i. Facilitate formulation and review of the ICT strategies, policies, procedures, guidelines and plans which ensure cost-effective application and management of UETCL's ICT systems and resources in accordance with the CBP.

ii. Review current and future ICT technologies to identify opportunities to increase the efficiency of ICT resources.

iii. Monitor and evaluate ICT projects and achievements against the ICT Strategic Plan.

iv. Inform and make recommendations to the MD/CEO and Board of the UETCL's significant ICT issues.

6.3 Steering Committee Responsibilities

The responsibilities of the ICT Steering Committee are to:

i. Ensure that ICT strategies, policies, procedures and guidelines are developed and aligned with the UETCL's strategic and corporate objectives as set in the CBP.

ii. Direct the development and authorization of the UETCL's ICT strategic and operational plans and recommend the same to the MD/CEO for approval.

iii. Review, prioritize and approve ICT strategic initiatives, projects and business cases and their respective budgets to ensure that ICT resources are optimized.

iv. Review and approve the detailed ICT project implementation plans and project management documents such as information risk management and information security.

v. Improve on the quality, management and value of ICT systems.

vi. Monitor and ensure that the ICT Strategic Plan is delivered within the agreed budget and timeframe.

vii. Monitor and report on the implementation of ICT projects and initiatives against approved project plans.

viii. Provide the MD/CEO with quarterly progress reports on the implementation of the ICT Strategic Plan initiatives and projects, as well as advising on current ICT issues and developments.

6.4 Procedures and Controls

6.4.1 Nomination

The head of department shall nominate a staff member who will then be approved by the MD/CEO.

Each department shall send one member to the committee

In case a member from a given department seizes to be for any reason, the chairman shall inform the head of department who then shall nominate a replacement within one month.

6.4.2 Steering Committee Term of office

The term of office of the Steering Committee shall be three years renewable.

6.4.3 Steering Committee meetings

The ICT Steering Committee shall meet at least once quarterly in each calendar year to discuss issues concerning ICT Policies and Strategy implementation, ICT policy guidelines and any other issues affecting the ICT function.

The quorum for the Steering committee shall be half of the members (50%) present.

The Committee shall, on behalf of management, propose strategic recommendations on implementation of ICT Policy and Strategy and any other recommendations from ICT department on any key ICT issues affecting ICT function subjected to Management approval.

7 ICT system acquisition policy

7.1 Policy

In order to align ICT requirements to the UETCL business, acquisition of all ICT systems shall be approved by the manager ICT in consultation with the Steering Committee requirements and advice.

7.2 Objective

i. To ensure that all systems acquired are aligned with the CBP, key focus areas and the prevailing technology trends.
ii. To avoid uncoordinated acquisition of ICT systems
iii. To ensure that all ICT systems acquisitions follow the appropriate approvals
iv. To avoid ICT systems duplications and unnecessary redundancies
v. To ensure timely acquisition of ICT equipment, software and/or services to avoid system interruptions.
vi. To identify and manage third party risks

7.3 Scope

This policy applies to all ICT system acquisitions and the related components particularly the following;

i. Equipment/Hardware/Devices and accessories
ii. Software/Systems/Applications
iii. Services
iv. Licenses

7.4 Responsibility

7.4.1 The Principal Information Technology Officer

Shall be responsible for the following;

i. Ensuring that the IT systems are budgeted for as per prevailing ICT strategy
ii. Ensuring that the IT systems specifications or TOR are complete and appropriate in accordance with industrial standards and that the concerned user requirements have been incorporated.
iii. Ensure timely identification, initiation and approval of IT systems needs
iv. Carrying out a User needs assessment

7.4.2 The Principal Communication Engineer

Shall be responsible for the following;

v. Ensuring that the telecom systems are budgeted for as per prevailing ICT strategy

vi. Ensuring that the telecom systems specifications or TOR are complete and appropriate in accordance with industrial standards and that the concerned user requirements have been incorporated.

vii. Ensure timely identification and initiation of telecom systems needs

7.4.3 The Principal Control Engineer

Shall be responsible for the following;

i. Ensuring that the power control systems needs are budgeted for as per prevailing ICT strategy

ii. Ensuring that the power control systems specifications or TOR are complete and appropriate in accordance with industrial standards and that the concerned user requirements have been incorporated.

iii. Ensure timely identification and initiation of power control systems needs

iv. MICT is responsible for ensuring timely submission and adherence to the annual procurement plans

v. MICT is responsible for ensuring all ICT system acquisitions are for systems that have been discussed and approved by the steering committee.

7.5 Procedures and Controls

i. The PPDA guidelines shall be followed while executing ICT systems acquisitions

ii. ICT systems acquisitions shall be triggered by the following;

   a. ICT strategic initiatives as stipulated in the ICT strategy
   b. Approved procurement plans
   c. Urgent user requirements upon approval by the head of the user section and/or the HOD depending on the threshold of funds required as per the FPPM.
   d. Urgent technical occurrences that must be solved for ICT systems to be stable. This shall be upon approval by the head of the user section and/or the MICT depending on the threshold of funds required as per the FPPM.

iii. User requirements shall be solicited through documented interactive sessions or filling of Form 11 appended to this document. The Form shall be signed by the head of the user section and PITO (for IT requirements), P. Com Eng. (for communication requirements) or P. Ctrl Eng. (for Control requirements).

iv. All specifications or Terms of Reference for communication systems shall be approved and signed off by P. Com. Eng to ensure fitness of purpose.

v. All specifications or Terms of Reference for IT systems shall be approved and signed off by PITO to ensure fitness of purpose.

vi. All specifications or Terms of Reference for Power Control systems shall be approved and signed off by the P. Ctrl Eng to ensure fitness of purpose.

vii. The FPPM shall be followed for emergency acquisitions

viii. Compatibility with existing systems shall be adhered to for all ICT systems acquisitions.

ix. Applicable international and industrial standards shall be followed during the preparation of specifications and terms of reference.

x. All ICT vendors, suppliers or contractors contracted to supply and install ICT systems shall be required to present an operational security management plan for approval by the contract manager, clearly indicating the following;

a) Identified critical areas or information
b) Analysis of threats
c) Analysis of vulnerabilities
d) Assessment of risk
e) Application of appropriate counter measures

xi. The contract manager of any ICT systems project shall closely monitor the contractor's compliance to the above operational security management plan.

8 ICT Systems Access

8.1 Policy

Access to all ICT systems shall require approval and/or Authentication.

8.2 Objective

i. Protect the ICT systems from intruders

ii. For proper implementation of the CIA triad. i.e. Confidentiality, Integrity and Accountability in relation to ICT systems

8.3 Scope

This policy applies to ICT systems and installations both operational and commercial. Specifically, the following;

i. ICT systems and installations

ii. Data Centres, Server Rooms and/or gazetted areas housing ICT installations

iii. Protected ICT devices and equipment

iv. National Control Centre

v. Splicing points on overhead fibre and Inspection manholes for the underground fibre

8.4 Responsibility

i. MICT is responsible for the overall ICT systems access.

ii. PITO is responsible for the day-to-day IT systems access control and access risk management.

iii. P. Com Eng. is responsible for the day-today telecom systems access control and risk management.

iv. P. Com Eng. shall be responsible for access to the main and auxiliary power supplies for the communication systems.

v. PITO shall be responsible for access to the server room and the rooms housing the power supplies for the IT equipment.

vi. P. Ctrl. Eng. shall be responsible for access to the National Control Centre's and the control rooms at the substations.

8.5 Procedures and Controls

8.5.1 Access Control

i. All premises housing ICT systems shall be fitted with centralized automated access control systems to track and manage entry.

8.5.2 ICT Technical Staff

i. ICT Technical staff refer to staff of UETCL employed within the department of ICT or Control section and assigned responsibilities of maintaining different components of the ICT systems.

ii. Each ICT technical staff shall be assigned sets of access credentials to cater for segregation of duties. One set of credentials shall be for access to systems as the experts and the other set of credentials for access to systems as an ordinary user.

iii. Upon being assigned the task to man a particular ICT system, Form 13 shall be duly filled and approved by PITO and MICT for IT systems, PCE and MICT for communication systems and P. Ctrl Eng. and MO&M for power control systems.

iv. A copy of the fully authorized Form 13 shall be forwarded to P. Ctrl Eng. for user creation and assignment of appropriate access rights to the power control systems, PITO for creation and assignment of appropriate access privileges to the IT systems and P. Com. Eng. for creation and assignment of appropriate access privileges to the communication systems.

v. PITO shall spear head the review of the assigned access rights monthly to ensure users continue to possess the assigned rights, nothing less and nothing more unless otherwise reassigned following this policy.

8.5.3 ICT Systems Guests

i. ICT system guests refer to authorized and/or official visitors to the premises within the jurisdiction of ICT department or control section with intensions of benchmarking, auditing, attending procurement related site visits, training, performing proof of concept or non ICT department staff on any such special assignment.

ii. Non UETCL staff that officially need temporary access to the whole or part of the ICT systems such as internet or telephony services shall also be categorised as ICT systems guests.

iii. Each guest shall be assigned temporary access credentials to enable them pursue their official mission and only for the authorized duration.

iv. Upon presenting their objectives and obtaining approval from the MICT, Form 13 shall be duly filled and approved by PITO and MICT for IT systems, PCE and MICT for communication systems and P. Ctrl Eng. and MO&M for power control systems.

v. A copy of the fully authorized Form 13 shall be forwarded to P. Ctrl Eng. for user creation and assignment of appropriate access rights to the power control systems, PITO for creation and assignment of appropriate access privileges to the IT systems and P. Com. Eng. for creation and assignment of appropriate access privileges to the communication systems.

8.5.4 ICT Internship Students

i. ICT Internship student refers to a student of a higher institution who applies and is granted permission to undergo practical training in the ICT department or control section for a specific period as part of the official institutions program.

ii. Each ICT internship students shall be assigned temporary and limited access credentials to enable them pursue their official mission and only for the authorized duration. Internship students shall only have access to the guest network.

iii. Upon presenting their applications and obtaining approval from the MHRA, Form 13 shall be duly filled and approved by PITO and MICT for IT systems, PCE and MICT for communication systems and P. Ctrl Eng. and MICT for power control systems.

iv. A copy of the fully authorized Form 13 shall be forwarded to P. Ctrl Eng. for user creation and assignment of appropriate access rights to the power control systems, PITO for creation and assignment of appropriate access privileges to the IT systems and P. Com. Eng. for creation and assignment of appropriate access privileges to the communication systems.

8.5.5 New Staff

i. PHRO shall ensure that the new staff fills in ICT Form7 attached to this document.

ii. The form shall be approved by MHRA and MICT

iii. A copy of the fully authorized Form 7 shall be forwarded to PITO for user creation and assignment of appropriate access rights on the IT systems

iv. A copy of the fully authorized Form 7 shall be forwarded to PCE for user creation and assignment of appropriate access rights on the telecom systems

v. A copy of the fully authorized Form 7 shall be forwarded to P. Ctrl Eng. for user creation and assignment of appropriate access rights to the power control systems.

8.5.6 Support Personnel

i. Support personnel shall mean the technical staff of a contracted firm assigned to perform technical assignments on behalf of the contractor.

ii. Support personnel shall be recognized as long as the contract between UETCL and the contractor is still valid.

iii. The contractor shall fill in Form 14 to indicate the personnel that shall be attached to UETCL as far as the said contract is concerned.

iv. For scheduled works a minimum of two days' notice shall be given by the contractor to UETCL detailing the personnel and the targeted ICT system components by filling in Form 14.

v. For scheduled works that shall interrupt ICT services, access shall only be granted outside UETCL working hours or at such times where interruption shall be deemed to have the least impact.

vi. For emergency works Form14 shall be filled retrospectively but in any case not later than 24 hours after completion of the task.

vii. The Form 14 shall be approved by PITO for IT systems, P. Comm Eng. For communication systems and P. Ctrl Eng. For power control systems.

viii. Support personnel shall be given system passwords with privileges and duration commensurate with the support task. Thereafter the password shall immediately expire and the account disabled.

8.5.7 Commercial Clients

i. Commercial client shall refer to a firm that has contracted UETCL to lease dark fibre, capacity, collocation or any other ICT service.

ii. Commercial clients shall be recognized as long as the contract between UETCL and the client is still valid.

iii. Access control systems shall be installed on all premises hosting commercial clients' equipment.

iv. The commercial client shall fill in Form14 to indicate the names of the technical persons that shall be attached to UETCL as far as the said contract is concerned.

v. For scheduled works a minimum of two days' notice shall be given by the client to UETCL detailing the personnel and the targeted ICT commercial components by filling in Form 14.

vi. For emergency works Form 14 shall be filled on site just before execution of the task and approval given there and then.

vii. The clients' personnel shall be given access passwords with pre-determined expiry to limit their stay in the restricted rooms.

viii. The clients' personnel access shall be restricted to the said clients' equipment only.

8.5.8 Access Revocation

8.5.8.1.1 System Access Revocation from Staff

i. Upon termination of employment and submission of an approved HR employment termination form, access to all ICT Systems shall be revoked from the affected staff member.

ii. Upon employee redeployment, access to all ICT Systems related to the previous position shall be revoked. Form 7 shall then be submitted to MICT for the new position.

iii. Access to part or entire requisite ICT system shall be revoked from a staff member upon writted notification by the HOD through MHRA and MICT in case of; indisciplene, gross incompetence, fraud and/or misuse.

8.5.8.1.2 System Access Revocation from Support personnel.

i. Upon premature termination of contract and submission of formal communication (email, memo, etc..) by Company Secretary and confirmed by MICT, access to all ICT Systems shall be revoked from the affected support personel.

ii. The ICT system access shall be revoked from a support or commercial clients' personnel upon submission of a formal communication from the respective contractor or commercial client indicating withdrawal or elimination of the said personnel's name or credentials.

8.5.8.1.3 System Access Revocation from ICT System Guests and Internship Students

i. Upon premature termination of a guest visit or internship offer, formal communication shall be sent by MHRA and confirmed by MICT. The ICT system access shall then be revoked from the affected guest or intern.

8.5.9 Rooms and Restricted Areas

i. ICT rooms and restricted areas shall include the following;

   a. Server rooms
   b. Battery Rooms
   c. Telecom POP's
   d. Generator rooms
   e. ICT Cubicles and Racks

ii. All the above rooms, cubicles and racks shall be locked at all times.

iii. Access to all such rooms and restricted areas must be to only authorized persons (ICT staff, authorized clients or authorized support personnel)

8.5.10 Passwords

i. Access to all ICT systems shall be restricted using passwords, codes, biometric credentials or swipe technologies managed centrally.

ii. PITO, Pr. Com Eng. and Pr. Ctrl Eng shall be responsible for setting the password complexity standards to be adhered to by all ICT system users for the systems under each principal officer's jurisdiction.

iii. User accounts passwords shall be changed every after a period not exceeding 42 days.

iv. System account passwords shall be changed quarterly and/or whenever the admnistrator is changed or terminated whichever comes first.

v. Custody of critical systems account passwords shall be the responsibility of; PITO for IT, P. comm. Eng. for communication, P. Ctrl. Eng for power control systems.

vi. Users shall be held accountable for all actions performed under their User ID, codes, biometric credentials and/or passwords.

vii. Sharing of user account passwords is completely prohibited and shall be treated as a disciplinary matter in accordance with the HR manual (Staff rules and regulations)

viii. The principle of least privilege shall be adhered to while accessing ICT systems whereby any user, program, or process shall have only the bare minimum privileges necessary to perform its function.

ix. All ICT systems not in use for three consecutive months shall be declared idle to MICT by the principal officer in charge. Upon approval by MICT the said system(s) shall be shut down or disconnected from the production environment.

x. User accounts shall be declared idle upon exceeding one week of non-usage/inactivity and shall be disabled forthwith by the responsible principal officer.

8.5.11 System Logging and Monitoring

i. All ICT critical system logs shall be centrally stored and security access rights implemented on the storage location to prevent administrators from manipulating or deleting the logs.

ii. The minimum retention period for all system logs shall be one year. There after the logs shall be backed up and deleted form production environment.

iii. Events to be logged shall include but not limited to;

   a. log-on attempts - recording user IDs, dates/times, successes/failures of attempts.

   b. creation, amendment and deletion of data - recording User IDs, dates and times.

   c. access and use of IT all resources including but not limited to internet and Email usage and printer activities.

iv. All ICT systems (software applications and infrastructure) shall be actively monitored by installing security incident and event management solutions to cub the risk of abuse of privileged access and rights.

9 Internet and Intranet Use

9.1 Policy

i. UETCL shall provide controlled internet and intranet services to staff to facilitate them in carrying out their day-today business operations and research. The internet and intranet service shall only be used for official Company work during official working hours.

ii. Staff shall only be allowed a maximum of 10 GB per month for mobile internet use for home and field usage.

9.2 Objectives

i. Enforce the appropriate and/or optimum usage of company equipment, network and Internet access

ii. Protect both the business, the employee and the corresponding equipment from cyber risks.

iii. Protect the integrity of the UETCL information relayed on the intranet and internet platforms.

iv. Enhance secure communication and collaboration between/among internal and external stakeholders.

9.3 Scope

i. All employees shall be entitled to access the internet and intranet services

ii. This policy applies to all employees of UETCL with access to computers and the Internet.

iii. Internet services shall be provided either as fixed (on premise) and/or mobile.

iv. Internet services shall include;

- **a.** Surfing the web
- **b.** Email: both corporate and private
- **c.** Use of the public cloud

v. Intranet services shall include;

- **a.** UETCL Connect
- **b.** Budget information System
- **c.** Wayleaves information system
- **d.** Outlook (Anywhere and Web access)
- **e.** GIS
- **f.** Any other online system for internal operations

9.4 Responsibility

i. MICT shall be responsible for the overall ICT internet and intranet usage and risk management.

ii. PITO shall be responsible for the secure implementation and monitoring of the internet and intranet usage.

iii. P. Comm. Eng. shall be responsible for the connection of the UETCL WAN through provision of the appropriate communication links.

iv. The ICT system users shall be responsible and accountable, individually, for their actions both on the internet and intranet.

9.5 Procedures and Control

9.5.1 Internet

i. Users of the Internet shall comply with all existing national laws, policies and regulations.

ii. Internet access shall be limited to mainly job-related activities during working hours.

iii. The PITO shall be responsible for the monitoring and control of all corporate internet usage and traffic.

iv. The PITO shall be responsible for blocking all website access and downloads if they are deemed to be harmful to UETCL business.

v. Surfing of obscene and pornographic material is prohibited and punishable.

vi. Access to mobile and residential Internet services shall be upon approval by the MD/CEO with justification by the user through his/her departmental head.

vii. The user, section or department that requires mobile and residential internet shall request in writing to MICT with justification. If deemed justifiable, the head of section shall then write to MICT who reviews and forwards request to MD/CEO for approval.

viii. The MD/CEO shall appoint an Online Information Committee (OIC) to, among other responsibilities, maintain the content and layout of the intranet portal with the technical support from the ICT department.

ix. Un acceptable internet use shall include;

- Perpetrating fraud
- Pirating
- Hacking and accessing unauthorized websites.

x. Reloading of data for mobile and residential internet shall be the responsibility of MICT.

xi. Any data loading needed prior to the prevailing schedule shall be requested for in writing to the MICT for approval.

xii. All remote offices and substations connected to the UETCL fibre shall access internet via the corporate internet connection

xiii. In the event of internet outage, PITO shall inform staff as soon as possible.

xiv. There shall be a minimum of two corporate internet connections from two different ISPs, a main and backup.

xv. The mobile internet shall serve the role of a second backup internet connection when the central corporate internet and the first backup connections have gone off. Therefore, staff with mobile internet service shall move with their devices at all times to avoid stalling of key/critical operations such as EFT, BOU remittances, URA remittances, sending of dispatch information to key stakeholders, etc.

xvi. The company website shall be one of the modes of communication to UETCL stakeholders and shall be reachable through a secured URL https://www.uetcl.go.ug

xvii. The responsibilities for the maintenance of the company website shall be as follows;

a.	Content management	PPRO
b.	Technical Support and maintenance	PITO
c.	Overall oversight	OIC

xviii. The company website shall always be up to date.

xix. Any cyber incident that compromises the security of UETCL ICT systems or threatens to do so shall be reported by PITO, Pr. Com Eng or Pr. Ctrl (depending on the ICT component affected) to MICT who shall then assess and accordingly report to the National IT regulating bodies including NITA-U and CERT-UG through the MD/CEO. All to be done in a duration not exceeding 36 hours from the time of the incident.

9.5.2 Cloud Services

i. The following services shall be considered for secure public cloud hosting due to the requirement for very high availability and mobile access;

a. Storage

b. Applications and or software as a service

c. Email

d. Surveillance

ii. Where local cloud services do exist for a particular function, priority shall be given.

iii. Cloud services to the SCADA system shall be limited to only support.

9.5.3 Intranet

i. An intranet in this policy and procedures manual shall be taken to mean a private network contained within UETCL that is used to securely share company information and computing resources among employees.

ii. Users of intranet shall comply with all existing national laws, policies and regulations.

iii. Intranet access will be limited to only official UETCL activities.

iv. UETCL Management reserves the right to revoke acess to intranet, and any other related services in case of indiscipline and/or contravention of this policy.

v. Intranet services shall be published for remote access and tele computing only after the MICT and PITO have established that the services are secure.

vi. Workflow management on the intranet shall be the responsibility of PITO

vii. Responsible staff shall submit a written notice to PITO through MICT and MHR&A about their intension to be out of office on leave or any other duties, including who is to act in their position so that the workflows on the intranet can be re-directed.

viii. PITO shall redirect the workflows back to normal upon return of the officer in (vii) above. The return shall be officially communicated through the same channels as in vii above.

ix. PITO shall ensure that all web based intranet services are protected using appropriate encryption technologies and standards.

x. Responsibility for the major intranet applications shall be as follows;

a. **UETCL Connect:**	Application owner	OIC
	Home page;	PPRO
	Departmental Pages:	PPRO, HOD's & HOS's
	Overall Oversight:	OIC
	Technical Support:	PITO
b. **BIS:**	Application owner	MFAS
	Data Capture:	HOS
	Opening/Closing:	PBFO
	Data control:	PBFO
	Technical Support & Maintenance.	PITO
	Overall oversight:	MFAS
	Granting/Revoking permissions	PBFO
c. **WIS:**	Application owner	MPI
	Data capture:	PPO - SA
	Granting/Revoking permissions	PPO - SA
	Technical Support & licence mgt.	PITO
	Overall oversight	MPI
d. **DIS (EDMS)**	Application owner	MHRA
	Scanning	PAO
	Data capture	PAO
	Granting/Revoking permissions	PITO
	Technical Support& licence mgt	PITO
	Overall oversight	MHR&A

e. **Fleet Mgt System**	Application owner	MP&I
	Data capture	PSSE
	Touch Key Allocation	PSSE
	Reporting	PSSE
	Granting/Revoking permissions	PSSE
	Technical Support - IT	PITO
	Technical Support – Telecom	PCE
	Coordinator	MP&I
f. **Accounting Sys**	Application owner	MFAS
	Data Capture	PDSO
	Opening and closing periods	PBFO
	Chart of Accounts	PBFO
	Reporting	PBFO
	Granting/Revoking permissions	PDSO
	Technical Support & licence mgt	PITO
	Coordinator - Operations	MFAS
	Coordinator – Technical	MICT
g. **HR/Payroll System**	Application owner	MHR&A
	Data capture - HR	PHRO
	Data capture - Payroll	PDSO
	Opening and closing periods	PDSO
	Interfacing	PDSO
	Granting/Revoking permissions	PITO
	Technical Support& licence mgt.	PITO
	Coordinator - Operations	MFAS
	Coordinator – Technical	MICT
h. **GIS**	Application owner	MP&I
	Data capture	PPE
	Granting/Revoking permissions	PPE
	System Administration	PPE
	Technical Support& licence mgt	PITO

i.	**Call Center**	Overall Oversight – Operations	MP&I
		Overall Oversight – Technical	MICT
		Application owner	DCEO
		Data capture	PPO-SA
		Granting/Revoking permissions	PPO-SA
		System Administration	PITO
		IT Support& licence mgt.	PITO
		Coordinator – Operations	DCEO
		Coordinator – Technical	MICT
		Supervision of agents	PPRO/PPO-SA

10 End Point Security Policy

10.1 Policy

i. UETCL shall enforce the practice of securing endpoints or entry points of end-user devices such as desktops, laptops, and mobile devices from being exploited by malicious actors and campaigns. Measures shall be put in place to quickly detect, analyse, block, and contain all sorts of attacks.

10.2 Objectives

i. To provide comprehensive protection from sophisticated malware and evolving zero-day threats.

ii. To provide cybersecurity's frontline of defence against the UETCL private network

iii. To quickly detect, analyse, block, and contain attacks in progress

iv. To provide administrators with visibility into advanced threats to speed detection and remediation response times.

v. To keep end user devices productive and connected

vi. To ensure fewer security incidents

vii. For easier deployment of complementary features or products

viii. For faster response to unwanted activity on the UETCL network

10.3 Scope

i. This policy applies to all end user devices for both internal and external stakeholders.

ii. End point devices shall include; Laptops, Tablets, Mobile devices, Smart watches, Printers, Servers, UPS's, Cloud based systems, IoT Devices, network devices and wearables.

10.4 Responsibilities

i. The Manager ICT shall be responsible for the overall security and risk management of end point devices

ii. The PITO shall be responsible for implementing security controls on end point devices and monitoring and thereafter training and sensitizing end users about the set controls and related trends from time to time.

iii. Pr. Comm Eng. shall be responsible for implementing security controls on end point devices for telecom system and monitoring and thereafter training and sensitizing end users about the set controls and related trends from time to time.

iv. Pr. Ctrl Eng. shall be responsible for implementing security controls on end point devices for Power control systems and monitoring and thereafter training and sensitizing end users about the set controls and related trends from time to time.

v. ICT system end users shall be liable, in their individual capacities, for abuse of end point security controls at their work stations.

10.5 Procedure and Control

i. UETCL shall deploy an integrated endpoint protection platform, which enables total visibility, response, and remediation.

ii. UETCL ICT network shall be fitted with a centralized end point protection platform with the following key features;

   a. Monitors the enterprise network as a whole and can offer visibility of all connected endpoints from a single location using agent based technology.

   b. With centralized administration capable of remote endpoint administration and configuration

   c. Automatic updates using technologies such as behavioural analysis

   d. Ability to remotely and centrally monitor employee devices, activity and behaviour

e. Device Firewalls
f. Email-Specific Antivirus Tools
g. Internet Security and Filtering
h. Mobile Device Management
i. Mobile Security Solutions
j. Application Controls
k. Encryption
l. Intrusion Detection Tools

iii. The end point protection platform shall be kept up to date at all times

iv. The endpoint protection platform shall include tools for monitoring every type of OS on the ICT network.

v. The centralized endpoint protection platform shall provide for insight into the security of the data assets and critical system files by providing controls for the following parameters; Data Encryption, Network Segregation, Data Loss Prevention, Data Access Governance File Integrity Monitoring.

vi. The end point protection platform shall be kept optimized at all times. That is to say it shall always be continuous and effective, integrated, proactive, usually automated.

vii. The end point protection platform shall be capable of detecting sudden abnormalities in end user behaviour, malicious file content, or other risks and trigger notification to the ICT security personnel and also keep a visible alarm/alert on the system.

viii. The endpoint protection platform shall enforce endpoint compliance by providing comprehensive client provisioning measures and assessing the device posture for all endpoints that access the network.

ix. Endpoints shall be continuously monitored for authentication, authorization, accounting (AAA), posture, and profiler.

x. Any device not complying with the set endpoint protection platform standards shall be denied access to the network. E.g. device with antivirus that is not up to date.

11 Online transaction system use

11.1 The policy

All UETCL key processes shall be done through secure online information systems.

11.2 Objectives

i. To enhance operational efficiency
ii. To reduce use of paper and save cost
iii. To reduce on process turnaround time and avoid unnecessary delays
iv. To enhance visibility and transparency as the online systems clearly indicate the status of the transaction to all stakeholders at all times.

11.3 Scope

i. This policy shall cover all online processes especially those that cut across business units (Departments).
ii. Particularly the following processes shall be handled through online transaction systems;
   a. Human Resource Management
   b. Projects implementation, monitoring and evaluation
   c. Engineering planning, operations and maintenance
   d. Financial processes
   e. Procurement processes
   f. Public and stakeholder communication

11.4 Responsibility

i. DCEO shall be responsible for launching any new online process companywide by formally notifying staff and/or external stakeholders where applicable.
ii. MICT is responsible for the overall online systems transaction security and risk management
iii. PITO is responsible for the planning, designing, implementation and monitoring of the online processes and the underlying security controls.
iv. The senior officers (Heads of Units), Heads of Sections and Heads of Departments shall review, advise, approve all online requests under their jurisdiction.
v. The CEO and/or DCEO shall approve online transactions where applicable or as stipulated in the relevant policy documents.

11.5 Procedure and Control

i. The online process shall only be accessible to the authorised personnel in the requisite business units.

ii. Once an online process has been approved and launched, all manual processes shall no longer be acceptable save for approved emergencies.

iii. Approval of requisitions within the online system shall be in harmony with the limits set in the existing policies, manuals, regulations and standards.

iv. In the event of official absence from duty, of an approver, the person who will be absent should write to MICT of a formal replacement prior to leaving office. MHR&A will be in copy of the communication.

v. PITO shall implement the online approval replacement in (iv) above within 12 hrs upon receipt of the written instruction.

vi. The substantive approver shall be reinstated into the online system upon confirmation of return to office by MHR&A through MICT.

vii. Approvers shall not delay with user requests for more than two working days.

viii. In the event of delayed action for more than two working days, the online system shall automatically notify the next approver.

ix. Approvers shall not continue to approve online requests when they are officially out of office unless with special permission approved by MICT.

x. Emergency workflow changes shall be approved by PITO in consultation with MICT.

xi. An approver shall not change any parameters on any given online request. If they do the request shall abort and require to be resubmitted.

12 Website Policy

12.1 The Policy

i. UETCL shall provide its stakeholders with an up-to-date company website as a medium of information dissemination, marketing and building corporate image.

12.2 Objectives

i. To educate and/or inform the public about UETCL's position in the energy sector, its vision, mission and core objectives.

ii. To disseminate accurate and up-to-date information to UETCL stakeholders

iii. To market the UETCL commercial businesses

iv. To build an attractive corporate image

v. To keep the UETCL stakeholders informed about the core activities and progress on major projects.

vi. To solicit feedback from stakeholders

vii. To act as a medium of advertisement for opportunities such as job placements and procurements.

12.3 Scope

i. This policy applies to the design, security, hosting and content management of the company website.

12.4 Responsibility

i. The CEO shall be responsible for vetting and approving content before it is published on the company website.

ii. MICT is responsible for the overall website availability, security and risk management

iii. The OIC shall be responsible for the overall design, content monitoring and quality control

iv. PPRO shall be responsible for the day to day update of vetted and approved content on the website.

v. PITO shall be responsible for website technical support and maintenance.

12.5 Procedures and Control

i. Any changes to the website, its layout or content shall only be uploaded upon approval by the MD/CEO.

ii. Maintaining of the UETCL website shall be done by PITO in consultation with the OIC and MICT

iii. Outdated information shall be immediately removed from the website, by the PPRO. In any case not later than one working day.

iv. The OIC shall assess the quality of the website content monthly and make recommendations for PPRO to implement in liaison with PITO.

v. The OIC shall assess the quality of the design and general layout of the website bi-annually and make recommendations for PITO to implement.

vi. The PPRO shall update the website on a daily basis where applicable.

vii. All approved information destined for the public shall appear on the company website as well.

viii. The PPRO shall respond to website based inquiries not later than one working day.

ix. The website shall always have a disclaimer.

x. The website must be up to date, informative and interactive to both internal and external stakeholders with all relevant information but particularly the following content must always be included and regularly updated;

1. Company mission, vision and objectives
2. The UETCL licenses
3. Ongoing, planned and completed projects
4. Fibre business information
5. UETCL related news i.e. commissioning of plants, CSR programs, etc.
6. Administrative information i.e. The Board, management team, organisation structure, etc.
7. Power systems control and dispatch information
8. Annual Audited accounts
9. Business related periodic reports (Monthly, quarterly, annual)
10. Picture gallery for UETCL activities
11. Job vacancies, if any
12. Open Tender adverts and best evaluated bidders’ notices
13. Links to UETCL social media accounts
14. Links to other stakeholders in the power sector
15. Provision for website visitors to provide feedback and/or make enquiries
16. Grid status and any planned, ongoing and completed grid reinvestment projects

13 Email Policy

13.1 The policy

i. UETCL shall provide electronic mail services with utmost security and privacy to its staff to facilitate them in official corporate business communication.

13.2 Objectives

i. To provide a secure and effective medium of communication for staff that uniquely identifies the UETCL domain.

ii. To securely disseminate critical business information to both internal and external stake holders

iii. A formal and acceptable means of notifying staff about tasks due for their attention and action. Could be from external stakeholders or internal stakeholders or online processes.

iv. To save costs by promoting a paperless environment.

13.3 Scope

i. This policy applies to all OFFICIAL email from the UETCL exchange server and external stakeholders.

13.4 Responsibility

i. Users/staff shall be fully responsible and accountable for the emails sent under their account.

ii. MICT shall play the oversight role for the email platform and its operations.

iii. PITO shall be responsible for the security, setup and availability of the email service.

iv. MHR&A shall be responsible for enforcement of ethics and etiquette on the email platform.

13.5 Procedure and Control

i. All employees of UETCL shall receive an e-mail account.

ii. The email naming convention shall be "***firstname.lastname@uetcl.com***"

iii. All email users shall be expected to use the service responsibly and productively.

iv. A newly recruited staff shall only be allocated an e-mail account upon full approval of their form 7:

v. Upon written approval by the MD/CEO, UETCL reserves the right to monitor mail content and usage for purposes of security or investigation-related reasons.

vi. Email communication shall comply with the corporate communication policy.

vii. PITO shall be responsible for securing the email platform.

viii. All corporate emails shall be accompanied by a standard disclaimer and a signature that includes Name, Title, mobile and fixed telephone contacts.

ix. Editing of the email disclaimer and header by a user shall be prohibited.

x. Emails sent using the company email system shall not contain offensive, defamatory, discriminatory, racist or with any harassing undertones.

xi. The company email system shall not be used to incite unlawful protests and disorder.

xii. Users shall not send or post chain messages, private solicitations, or advertisements that are not related to UETCL business or Corporate Social Responsibility activities.

xiii. The use of UETCL email shall be recognized as an official mode of communication.

xiv. MICT shall ensure users are trained and or sensitized continuously on issues pertaining email security.

xv. Users shall not send UETCL official information via mail to any third parties (outside UETCL) especially to the press/media without written authorization by the DCEO.

xvi. The control above excludes procurement related mails such as pre-bid and negotiation minutes as authorized by PPDA.

xvii. Users sending emails to fellow staff with storage intensive attachments (> 5mb) shall be required to use hyperlinks as opposed to attachments in order to save storage space on the network.

xviii. Upon leaving the company, a user's email account shall be immediately disabled by PITO upon receipt of written notification from MHR&A through MICT.

xix. PITO shall ensure all user emails are backed up and archived regularly to avoid loss of critical business communication records.

14 Software maintenance policy

14.1 The policy

i. All company software shall be maintained in accordance with approved user requirements and/or the Original Equipment Manufacturer OEMs' latest recommendations and industry best practices.

14.2 Objectives

i. To ensure continued software relevance and usability

ii. To comply with international software IT standards, trends and best practice

iii. To enhance the software security and that of the network.

iv. To optimally utilize the software and ensure value.

v. To allow for information categorization and clasification

14.3 Scope

i. This policy applies to both tailor made and off the shelf software

ii. The policy also applies to both OT and IT software

iii. The policy applies to the software applications and the information generated therein

14.4 Responsibility

i. MICT shall be responsible for the overall software planning, budgeting, maintenance, security and risk management.

ii. MICT shall perform the responsibility in (i) above in coordination with the application owners as specified in 13.4 (vi) below.

iii. Application owners shall also play the role of owners of the information asset for the information generated by the application software under their jurisdiction and shall be accountable for this asset category.

iv. PITO shall ensure that all software is always licensed and up to date.

v. For OT, PITO shall perform the responsibility in (iii) above in coordination with the following;

a. P. Ctrl. Eng. for OT software relating to power system control
b. P. Com. Eng. for OT software related to telecom systems
c. P. Planning Eng. for OT software related to power system planning
d. P. Protection Eng. for OT software related to power system protection and metering
e. P. Maintenance Eng. for OT software related to power grid operations and maintenance

vi. PITO in collaboration with the application owners or their delegates shall periodically assess the need for functional improvement.

vii. Any functional application improvements shall require the approval of the application owner and MICT before submission to the steering committee for final approval.

viii. Application owners for the running applications and/or systems (together with the information generated therein) shall be as follows;

No.	Application/System	Owner	Remarks
1.	Financial Applications	MFAS	e.g. Sun, BIS, Billing
2.	Power system Control	MO&M	e.g. SCADA, PMA
3.	Power system planning	MP&I	e.g. PSSE, Digisilent
4.	Computer Aided Design (CAD)	MP&I	e.g. Civil/Structure, Electrical, Mechanical and Architectural CAD
5.	Survey and GIS	MP&I	
6.	Power system protection and metering	MO&M	e.g. Relay Management. AMI
7.	Human Resource management	MHR&A	e.g. Payroll, Human Capital Management-HR module, Time and attendance
8.	Audit Management Systems	MIA	e.g. Teams, ACL

No.	Application/System	Owner	Remarks
9.	Fleet Management	MP&I	
10.	Land Acquisition and Compensation System	MPI	e.g. WIS
11.	Surveillance and access control	MCS	
12.	Public Relation Systems	DCEO	e.g. Call Centre management system, Company Website
13.	Electronic Document Management	MHR&A	
14.	Back Office ICT Systems	MICT	e.g. Databases, Firewalls, Mail systems, NOS, Antivirus etc.
15	Board Management Systems	CS	e.g. E-board
16.	Telecommunication management Systems	MICT	e.g. Foxman, OmniPCX,

14.5 Procedure and Control

i. Any modifications and/changes to a tailored software shall be documented and approved by MICT and the application owner.

ii. All requirements for software patches shall be reviewed, tested and approved by the PITO prior to their prompt deployment.

iii. All Major. (Quantified by man hours) Software enhancements and/or decommissioning of part or the whole software shall be justified by the application owner, PITO and approved by MICT before submission to the ICT Steering Committee for final approval.

iv. Any decommissioned software shall remain accessible (with Minimum functionality) for viewing purposes for at least one year after commissioning of the new software.

v. MICT and the application owner shall manage the acquisition lead times for any new software to avoid service disruption.

vi. PITO and the application owner shall ensure that any new software acquired shall include training for both technical and the intended users.

vii. For any new software, upgrades and/or enhancements, user manuals and system documentation must be submitted by the vendor to PITO and the application owner.

viii. PITO and the application owner shall ensure that any new software acquired shall include a service level agreement for support and maintenance covering at least one year.

ix. MICT together with the application owner shall approve the installation of software on equipment owned by UETCL using ICT Form 6.

x. PITO shall ensure regular patching of software in tandem with the OEM schedule of patch releases. Procedure (iii) above does not apply to patches.

xi. PITO shall ensure Patches are tested before deployment into production

xii. Software in use on the UETCL systems shall not be at least two (2) releases older than the latest version.

xiii. PITO shall be the custodian of all installation media and shall maintain a database of all installed production software.

xiv. Software installation shall be done in accordance with the Original Equipment Manufacturer's manuals.

xv. New software installation and upgrades shall be managed in such a way that there is none or minimal disruption to normal business operations. Deployment of upgrades to production software shall follow the parallel run approach until stability of operations has been attained.

15 Software licensing, installation and copyrights policy

15.1 The policy

i. All software to be installed and used on UETCL ICT systems shall be properly licensed by the respective author(s) with accurate and up-to-date licences.

15.2 Objectives

i. To ensure total license compliance and fulfil UETCL obligations under the Ugandan copyright law
ii. Avoid licensing penalties due to violation
iii. To encourage the development of culture, science and innovation, while providing a financial benefit to copyright holders for their works, and to facilitate access to knowledge.
iv. To provide employees with a uniform approach to addressing licensing and copyright issues

15.3 Scope

This policy shall cover the following software types;

i. Off shelf software developed by OEMs
ii. Custom developed software. Both in house and outsourced.

15.4 Responsibility

i. MICT shall be responsible for the overall software licensing and copyright protection.
ii. MICT shall be responsible for budgeting for all the software in UETCL in coordination with application owners.
iii. PITO shall be responsible for the implementation and technical support for software licenses.
iv. Application owners shall be responsible for reporting license renewal, increase or decrease requirements to PITO through MICT in a timely manner to avoid service disruption.
v. PITO will have the responsibility to ensure that licences are renewed in a timely manner.

15.5 Procedure and Control

i. UETCL shall use only licensed software and or copyrighted. Pirated software shall not be installed on UETCL ICT systems. (Not applicable to open source software).

ii. Unless otherwise provided in the applicable license, notice, contract, or agreement, no copyrighted software shall be duplicated, except for backup and/or archival purposes.

iii. Records of all software licenses owned by the company shall be maintained and licenses monitored in such a way that their respective renewals are initiated and concluded before expiry of the subject licenses.

iv. All users of ICT systems shall comply with the Ugandan laws of intellectual property.

16 Change Control Policy

16.1 The Policy

All changes to Corporate ICT systems shall be requested for by the user/application owner and approved by the Manager ICT in consultation with the Steering Committee for corporate ICT systems.

16.2 Objectives

i. To respond to the change requirements while maximizing value and reducing incidents, disruption and re-work.

ii. To respond to the requests for change that will align the services with the business needs.

iii. Ensure that changes are recorded and evaluated, and that authorized changes are prioritized, planned, tested, implemented, documented and reviewed in a controlled manner

iv. Ensure that changes to configuration items[1] are recorded in the Configuration Management System

v. To mitigate overall business risk

[1] A configuration item refers to any element that needs to be controlled in order to deliver a service. It can be a software e.g. sun system.

16.3 Scope

i. Change management shall cover all critical ICT systems. A critical ICT system refers to one that affects UETCL operations directly and significantly such as the SCADA system and the email service.

ii. Any activities affecting the following areas or their related components shall undergo the change management process;

a) Critical ICT services
b) Configuration items
c) ICT processes
d) System documentation
e) Hardware setup
f) System designs
g) Software development platforms
h) Software application setup

16.4 Responsibility

i. MICT shall be responsible for all ICT systems related changes in coordination with the application owners.

ii. MICT shall perform the responsibility in (i) above in coordination with the application owners.

iii. P. Ctrl. Eng. shall be responsible for implementation and control of power system control related changes

iv. PITO shall be responsible for implementation and control of IT system related changes

v. P. com. Eng. shall be responsible for implementation and control of telecom related changes

vi. The steering committee shall play the role of a Change Advisory Board

vii. The Steering committee shall perform the roles of the Change Advisory Board as below;

a) Assessment of the risks and the consequences of besought changes and proposing appropriate mitigation measures.

b) Reviewing Requests for Change (RFCs) – bearing in mind the resources available and probable influence.

c) Provide strategic support and collaboration for the change process

d) Partaking in continuous improvement initiatives to the change management process.

16.5 Procedure and Control

i. All major changes to the critical ICT systems shall be implemented upon request by the application owner, approval by MICT and the change advisory board. A major change is an alteration in system configuration/setting/design whose consequence can lead to service disruption.

ii. Changes shall be justified, approved and original configurations/settings backed up for possible fall-back in case of unforeseen undesirable outcomes.

iii. The implementation of change shall be done in such a manner as to minimize or eliminate business disruption, in any case outside official working hours.

iv. PITO, P. Ctrl. Eng. and P. Com Eng. shall ensure that any system changes implemented within their jurisdiction and their respective technical effects are documented.

v. Overall system documentation must be updated accordingly.

vi. An emergency (fix-on-fail) change must comply with this policy and all related standards retrospectively.

vii. Change management records shall be kept in a change management software and all ICT change management stakeholders shall be trained accordingly.

viii. All critical ICT systems shall have an audit trail to track any changes made, when and by who.

ix. PITO, P. Ctrl. Eng. or P. Com Eng. shall issue system privileges and/or ability to execute changes in line with technical know-how and/or seniority.

x. All premises housing critical ICT infrastructure shall be fitted with surveillance and access control systems to track any physical changes to the infrastructure.

17 Acceptable use policy

17.1 The Policy

i. ICT systems shall be used for UETCL business purposes in compliance with all existing internal policies, National constitution, regulations and legislation by any legitimate authority.

17.2 Objectives

ii. To set the minimum common standards of ICT acceptable use in UETCL

iii. To provide guidance on proper usage and utilization of ICT systems and equipment to ensure usage up to expected life time

iv. To protect the rights and privacy of all employees

v. To protect the integrity and reputation of UETCL

vi. To establish specific requirements for the use of all telecom, computing and network resources at UETCL

17.3 Scope

i. This policy applies to all users of telecom, computing and network resources owned or managed by UETCL.

ii. Individuals covered by the policy include UETCL staff, students on internship training, UETCL guests or agents of the administration, external stakeholders and UETCL extranet users.

iii. Computing resources include all UETCL owned, licensed, or managed hardware and software. This includes devices connected to the network either physically or via wireless connection, regardless of the ownership of the device.

17.4 Responsibility

i. MICT shall be responsible for the overall protection of the UETCL ICT systems from abuse and intrusion.

ii. MICT shall perform the responsibility in (i) above in collaboration with application owners.

iii. MICT shall be responsible for sensitizing users, training and communicating any changes, additions and/or deductions in the ICT systems, policies and procedures.

iv. All ICT system users are responsible for knowing the regulations and policies of UETCL that apply to appropriate use of the company's technologies and resources.

v. Users are responsible for exercising good judgment in the use of the company's technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action.

vi. PITO, P. Ctrl. Eng., P. Com Eng shall be responsible for monitoring and reporting of unacceptable use of ICT systems under their jurisdictions to MICT or MO&M for further action in accordance with the UETCL staff rules and regulations.

17.5 Procedure and Control

i. ICT resources shall only be used by the authorised persons for the approved purposes in accordance with the ICT systems security policy.

ii. Super users and administrators of ICT systems shall respect the rights of others including protecting the privacy and security of all the data therein.

iii. All users of ICT systems are expected to respect the privacy and personal rights of others.

iv. ICT system shall not be used to monitor the activity of staff in any way without their prior knowledge save for cases of authorized investigations and auditing.

v. Staff shall promptly report any incidents of possible abuse or misuse of ICT resources, policy violations or weaknesses to MICT.

vi. The care for any ICT facility shall be vested in the user to whom it is allocated. The duty-of-care for the shared or general ICT equipment will be vested in Principal IT Officer, P. Ctrl. Eng. or P. Com. Eng. depending on the nature of the equipment.

vii. Users shall not leave their workstations unattended without either logging off or locking them.

viii. Users shall not transmit any information that may be damaging the reputation of other users, UETCL and its stakeholders; the use of ICT resources to libel, slander, or harass any other person is not allowed and could lead to disciplinary action and/or legal action.

ix. Personal use will normally be tolerated provided that:

a. It is occasional, reasonable and does not interfere or undermine UETCL work activities.

b. It does not create conflict of interest, violate any other UETCL policies or contravene the laws of Uganda.

x. UETCL reserves the right to access and review personal content under certain conditions. These may include: investigating performance deviations and system problems (with reasonable cause), determining if an individual is in violation of this policy, or, as may be necessary, to ensure that the company is not subject to claims of institutional misconduct.

xi. ICT will only create a user account upon receipt of acknowledgment of receipt of ICT policy by the user.

xii. The user has the responsibility to keep up-to-date on changes in the ICT environment, as published, during sensitization workshops, using electronic and print publication mechanisms, and to adapt to those changes as necessary.

xiii. Irresponsible use of ICT systems such as; Porn, excessive commercial calls, excessive live streaming shall be punishable following the Human resource manual.

18 Systems Administration Policy

18.1 The Policy

i. System Administration must be accomplished in a professional and timely way with a goal of protecting and maintaining the availability of UETCL ICT resources running on the ICT infrastructure throughout the organization to the tune agreed upon in the official ICT SLA.

18.2 Objectives

i. To protect and maintain the availability of UETCL information technology resources running on the ICT infrastructure throughout the organization to the level agreed upon in the official ICT SLA.

ii. To ensure that ICT systems configurations and installations comply with all technology policies, the ICT strategy, CBP and standards established by UETCL and global ICT frameworks such as COBIT and ITIL.

iii. Guide implementation of ICT policies and procedures governing access to, and use of, systems and technical services.

iv. To take precautions against theft of or damage to the system components and data, and to report such events to PITO, Pr. Ctrl, Pr. Com Eng and/or PSO when such events occur.

v. To treat information about, and information stored by, the system's users in an appropriate manner respecting privacy and confidentiality. The System Administrator's ability to access must not be confused with authority to access data.

vi. To understand the data elements stored in a system, the data classifications and to take precautions to protect the security of the ICT system and the privacy, confidentiality and quality of information contained therein.

18.3 Scope

i. This policy applies to all ICT personnel entrusted with privileged and superior system responsibilities and access rights exceeding ordinary system users.

ii. The policy applies to all UETCL ICT resources whether individually controlled or shared, stand-alone and/or networked.

iii. It applies to all ICT resources, including systems and servers, owned, leased, operated, and/or controlled by UETCL.

iv. The term systems administrator shall refer to the ICT personnel in ICT or O&M departments with privileged rights and mandate to maintain a given ICT system or its components.

18.4 Responsibilities

i. The Manager ICT shall be responsible for management of the entire ICT systems administration aspects.

ii. The PITO shall be responsible for implementing systems administration controls and risk mitigation measures for IT systems and related infrastructure and thereafter training and sensitizing systems administrators about the set controls and related trends from time to time.

iii. Pr. Comm Eng. shall be responsible for implementing systems administration controls and risk mitigation measures for Telecom systems and related infrastructure and thereafter training and sensitizing systems administrators about the set controls and related trends from time to time.

iv. Pr. Ctrl. Eng. shall be responsible for implementing systems administration controls and risk mitigation measures for Power control systems and related infrastructure and thereafter training and sensitizing systems administrators about the set controls and related trends from time to time.

18.5 Procedure and Control

i. When the System Administrator has reasonable cause for suspicion, s/he has the right to monitor any and all aspects of a user's activity to determine if the user is violating policies and putting the system at risk. This can include, but is not limited to: login sessions, files, surfing and e-mail.

ii. The System Administrator shall respect the rights to privacy of the users and will not engage in actions that will violate this without cause.

iii. The administrator will get consent to enter a user's account, in non-security and non-emergency cases, or request department head authorization to do so as necessary.

iv. The System Administrator has the responsibility to provide advanced notice of system shut down, through the head of section, for maintenance or upgrades, so that users may plan around the times of system unavailability. However, in the event of an emergency, the SA may shut down a system with little or no advanced warning.

v. The System Administrator shall not be liable for the actions that are technically deemed to be the responsibility of the users.

vi. Users shall be responsible for any and all activity from his/her account on the ICT system.

vii. Users shall be responsible for fair use of resources such as drive space, CPU time, printing, and other shared resources which are at their disposal upon login.

viii. It is the responsibility of the user to report problems (and requests) with ICT equipment via the help desk (preferred) or any other means at their disposal.

19 Database Administration policy

i. Data residing on ICT systems shall be managed as a UETCL critical resource. Data usage and data sources shall be managed through the stewardship principles of administering and controlling data quality and standards in support of UETCL Corporate objectives.

19.1 Objectives

i. To identify and manage up-to-date documentation on all database system hardware, software, and users.

ii. Installation, configuration and upgrading of database server software and related products.

iii. To establish and maintain sound backup and recovery policies and procedures.

iv. To evaluate database features, design and implementation.

v. To implement and maintain database security (create and maintain users and roles, assign privileges).

vi. Database tuning and performance monitoring.

vii. Application tuning and performance monitoring.

viii. To plan growth and changes (capacity planning).

19.2 Scope

i. This policy applies to all ICT personnel entrusted with privileged and superior database management responsibilities and access rights exceeding ordinary database users.

ii. The policy applies to all UETCL ICT databases whether individually controlled or shared, stand-alone and/or networked.

iii. A database administrator shall refer to the ICT officer with superior privileges and expertise and is officially mandated to utilize specialized software to store and organize data residing on ICT systems. The role shall include capacity planning, installation, configuration, database design, migration, performance monitoring, security, troubleshooting, as well as backup and data recovery.

19.3 Responsibilities

i. The Manager ICT shall be responsible for management of the entire ICT database administration aspects.

ii. The PITO shall be responsible for implementing database administration controls and risk mitigation measures for IT databases and related infrastructure and thereafter training and sensitizing database administrators about the set controls and related trends from time to time.

iii. Pr. Comm Eng. shall be responsible for implementing database administration controls and risk mitigation measures for Telecom databases and related infrastructure and thereafter training and sensitizing database administrators about the set controls and related trends from time to time.

iv. Pr. Ctrl. Eng. shall be responsible for implementing database administration controls and risk mitigation measures for Power systems databases and related infrastructure and thereafter training and sensitizing database administrators about the set controls and related trends from time to time.

19.4 Procedure and control

i. The primary ownership of a data set shall rest with the application owner of the underlying application generating the said data set.

ii. Authorization and data control: Access to the production (and replication) databases shall be restricted to production applications and through authorized reporting tools.

iii. Developers, internal or outsourced, shall have a special role for functional development and integration databases that they support.

iv. DBA shall provide support to the development group.

v. Support activities shall include, but shall not be limited to the following areas: database design or re-design; application design; application (SQL) performance analysis; disk space analysis; data recovery analysis; and data and process modelling.

vi. Operational support shall include: production application analysis; data monitoring and reorganization; recovery management; space management; performance monitoring; exception reporting; application system moves to production.

vii. The DBA shall bring application inefficiencies to the attention of the relevant application owner and make recommendations, if desired, on ways to tune them and make them more efficient.

viii. The DBA shall be responsible for backup and recovery of the databases under their jurisdiction in accordance with the overall UETCL ICT disaster recovery manual.

20 ICT Services Demand Management Policy

20.1 The policy

i. The use of ICT resources in UETCL shall be rationalized and optimized to ensure that the amount of technical and human resources that has been budgeted matches the expected demand for the available ICT service.

20.2 Objectives

i. To identify and analyse the patterns of business activity (PBA) in order to understand the levels of demand which will be placed on the ICT services.

ii. To analyse the profiles of the different users of each service so that the profiles of demand can be understood.

iii. To make sure that the ICT services are defined to meet the expected patterns of the entire UETCL business activity.

iv. To ensure that suitable resources are available to meet the demands of the ICT service.

20.3 Scope

i. ICT service demand management shall apply to all ICT services in UETCL as defined in this policy document

20.4 Responsibilities

i. The Manager ICT shall be responsible for the overall ICT services demand management.

ii. The PITO shall be responsible for IT services demand management and risk mitigation measures for IT services demand related infrastructure and setting the controls and related trends from time to time.

iii. Pr. Com Eng. shall be responsible for Telecom services demand management and risk mitigation measures for telecom services demand related infrastructure and setting the controls and related trends from time to time.

iv. Pr. Ctrl. Eng. shall be responsible for power systems services demand management and risk mitigation measures for power systems services demand related infrastructure and setting the controls and related trends from time to time.

20.5 Procedures and Control

i. The heads of section shall analyse the prevailing services usage within their jurisdiction by assessing the service desk data which contains details of incidents, requests, and problems and produce a quarterly ICT services demand report.

ii. The heads of section shall liaise with the users directly regarding the needs which have been predicted, analyse trends in usage and make educated projections regarding usage of the ICT services in the future based on similar user trends.

iii. It is the duty of the section heads (PITO, Pr. Com Eng or Pr. Ctrl Eng) to make sure that the appropriate costs are included in the ICT service design during planning and budgeting

iv. PITO, Pr. Com Eng and Pr. Ctrl Eng shall maintain an up to date service catalogue for the services under their jurisdiction. (Use the recommended ITIL service catalogue template).

v. The following record of user's ICT service usage shall be maintained by the heads of section for all the services under their jurisdiction;

  a. **Frequency:** It shows how often the volume of usage happens.
  b. **Duration:** It shows how long the business usage pattern lasts.
  c. **Location:** It shows where the business usage has occurred.

21 Software Design and development Policy

21.1 The Policy

i. Designing, Developing and/or implementing new ICT systems and software applications at UETCL shall be done in a controlled, predictable, consistent and efficient manner.

21.2 Objectives

ii. To ensure that systems development activities progress in a predictable and controlled fashion.

iii. To ensure review and testing at all levels of development and provide for approvals, security assessments, and change control management.

iv. To align information systems development activities with the overall UETCL strategic business goals.

21.3 Scope

i. This policy applies to all information systems development and all software and application development activities performed by and on the behalf of UETCL

21.4 Responsibilities

i. The Manager ICT shall be responsible for the overall ICT systems, software and application development management.

ii. The PITO shall be responsible for ICT systems, software and application development and risk mitigation measures and implementation of the controls and related trends from time to time.

21.5 Procedures and Control

i. All software developed in-house which runs on production systems must be developed according to the SDLC. At a minimum, this plan should include preliminary analysis or feasibility study; risk identification and mitigation; system analysis; general design; detail design; development; quality assurance and acceptance testing; implementation; and post-implementation maintenance and review.

ii. All developed software shall be adequately documented and tested before it is used for critical UETCL information processing.

iii. All production systems must have designated owners for the critical information they process.

iv. PITO shall perform annual risk assessments of production systems to determine whether the controls employed are adequate.

v. All production systems, software and/or applications shall have an access control system to restrict who can access the system as well as restrict the privileges available to these users.

vi. PITO shall assign an administrator for all production systems, software and/or applications to grant and revoke access according to guidelines in the Account Management Procedure.

vii. Where resources permit, there shall be a separation between the production, development, and test environments. This will ensure that security is rigorously maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions. Where these distinctions have been established, development and test staff must not be permitted to migrate code changes to production systems.

viii. All application-program-based access paths other than the formal user access paths must be deleted or disabled before software is moved into production.

22 ICT Deployment Policy

22.1 The policy

i. All ICT infrastructure, systems, applications and/or software deployments shall be planned, scheduled and controlled so as to build, test and deploy in order to deliver new functionality required by the UETCL business while protecting the integrity and continuity of existing services.

22.2 Objectives

i. To ensure continuity of ICT services despite the introduction of new releases and/or deployments.

ii. To create an environment within which infrastructure, system, application and/or software deployments are planned, scheduled and controlled.

iii. To create the assurance that new deployments will deliver the value and outcomes required to meet the set UETCL business goals.

iv. To create a clear communication and understanding of the risks associated with executing the deployments.

22.3 Scope

i. This policy applies to all ICT infrastructure, systems, applications and software deployments destined for the UETCL ICT production environment.

22.4 Responsibilities

i. The Manager ICT shall be responsible for the overall ICT deployment management including facilitation of the deployment process and ensuring an enabling environment.

ii. The PITO shall be responsible for implementing deployment management procedures, controls and risk mitigation measures for IT infrastructure, systems, applications and software deployments.

iii. The Pr. Com Eng. shall be responsible for implementing deployment management procedures, controls and risk mitigation measures for telecom infrastructure, systems, applications and software deployments.

iv. The Pr. Ctrl Eng. shall be responsible for implementing deployment management procedures, controls and risk mitigation measures for power system infrastructure, applications and software deployments.

22.5 Procedure and Control

i. Each deployment shall be designed and governed by a request for change raised via the change management process to ensure effective control and traceability.

ii. Deployments shall be planned and designed to be built, tested, delivered, distributed and deployed into the live environment in a manner that provides the agreed levels of traceability, in a cost effective and efficient way.

iii. All deployments shall require use of Development, Test, UAT and Pre-production before being released into the production environment.

iv. Major deployments shall be fully tested under a realistic load before they are deployed into production and the tests shall be documented.

v. Unless otherwise dictated by unforeseen technical circumstances, all deployments shall include a parallel run for a minimum of one month or until stability is guaranteed, whichever comes first.

vi. Emergency deployments shall be managed in line with the emergency change procedure and shall be reported as appropriate.

vii. Records shall be kept of planned release and deployment dates and deliverables with references to related change requests and problems. They will be used to record and manage deviations, risks and issues related to the affected service.

viii. All deployments shall be tracked, installed, tested, verified and/or uninstalled or backed. Exceptions will require approval.

ix. Knowledge transfer shall be enforced during deployments to enable the UETCL technical staff and users to optimise their use of the service to support their business activities.

23 Physical Security policy

23.1 The Policy

ii. There shall be adequate facilities and access controls to prevent damage, interference and unauthorized physical access to ICT installations.

23.2 Objectives

i. To ensure that ICT personnel are protected from harm and disaster.

ii. To ensure the physical security of ICT resources and data.

iii. To protect ICT premises from a range of physical security threats including crime, espionage, natural disasters and acts of terrorism.

iv. To minimise or remove the risk of the ICT network and/or its core components being rendered inoperable or inaccessible.

v. To ensure the enforcement of Confidentiality, Integrity and Accountability on the ICT network and/or its core components.

23.3 Scope

i. Physical security shall apply to buildings used in the processing and storage of ICT Information.

ii. The buildings referred to in (i) above shall include; data centres, node rooms, power system control centre, computing and telecom points of presence for UETCL and its clients.

iii. All ICT Assets (fixed or mobile) that store and/or or process information shall also be covered by this policy.

23.4 Responsibilities

i. MICT and MCS shall be responsible for the overall physical security of ICT systems and the related infrastructure

ii. The duo shall perform the responsibility in (i) above in collaboration with the ICT infrastructure end users.

iii. Users shall be responsible for the physical security of any ICT equipment allocated to them

iv. PSO in coordination with PITO, P.Com. Eng. and P. Ctrl. Eng. shall implement, monitor, control and report about the physical security for equipment and infrastructure under their jurisdiction.

v. PSO shall be responsible for continuous monitoring of the ICT facilities and supervision of the centralized surveillance system.

23.5 Procedure and Control

i. In all circumstances security of personnel shall always take precedence over any other system components.

ii. Authority for guests and/or non-technical staff to access sensitive ICT infrastructure such as server rooms, telecom POPs, control centres shall be granted by the PITO, P. Com Eng. or P. Ctrl. Eng. in their respective jurisdictions and a record maintained through ICT form 4.

iii. Sensitive ICT infrastructure shall be housed in rooms with strong doors and burglar proofs.

iv. In the event that the allocated ICT equipment is lost or stolen, the user shall immediately report to police and submit the report to MCS who shall in turn liaise with the MHR&A and MICT for any further actions to be taken in accordance with the UETCL staff regulations.

v. Physical access to all sensitive ICT premises shall be restricted using biometric access control systems, monitored by CCTV.

vi. Technical personnel shall document all activities carried out while in the ICT premises in the designated premises log book.

vii. Access to all sensitive ICT infrastructure by non-authorized personel is prohibited.

viii. Mobile devices such as laptops, PDA's, mobile phones shall not be left unattended and unsecured. Desk locking devices shall be provided where applicable.

ix. There shall be adequate safety measures such as fire suppression, UPS, earthquake and flood prevention systems installed in all sensitive ICT infrastructure areas.

x. Data centre sites shall be located strategically taking into consideration issues such as its visibility; proximity to hazards and crime; natural disasters; transportation; access to environmental controls and emergency services.

xi. UETCL shall apply physical security controls in accordance with US ISO/IEC 27001:2005;

xii. All visitors shall produce proof of identification before gaining access to sensitive ICT facilities. The visitors must sign-in and sign-out.

xiii. Guests, Users and non-technical personnel shall only know of the existence of, or activities within an ICT secure area on a Need-to-Know basis

xiv. Unless authorised for a business purpose, use of photographic, video, audio or other recording equipment, such as cameras on mobile devices in sensitive secure rooms are prohibited. Such devices shall be surrendered at the security desk when visiting secure areas.

xv. All rooms and sensitive data processing areas shall be fitted with controls to minimise the risk of potential physical threats, e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism

xvi. Eating, drinking, and smoking in proximity to information processing facilities is prohibited.

xvii. Environmental conditions, such as temperature and humidity which could adversely affect information processing facilities shall be monitored.

xviii. Power and telecom cabling shall be protected against interception or damage by installing lightning protection to all buildings and fitting lightning filters/surge arrestors to incoming power and communications lines.

xix. All media used to store and process sensitive information such as networking devices; magnetic disks and tapes; office equipment; solid state devices (SSDs); and optical disks shall be sanitised and disposed of securely.

24 System and Information Security policy

24.1 The Policy

i. UETCL shall implement controls to safeguard ICT applications and critical business information residing on the ICT systems through system access controls and privileges, prevention and detection of intrusion in line with the business requirements and the market industry standards.

24.2 Objectives

i. To establish a general approach to information security

ii. To detect and forestall the compromise of information security such as misuse of data, networks, computer systems and applications.

iii. To protect the reputation of the company with respect to its ethical and legal responsibilities

iv. To observe the rights of the users and stakeholders.

v. Providing effective mechanisms for responding to complaints and queries concerning real or perceived non-compliances.

24.3 Scope

i. This policy shall address all data, programs, systems, facilities, other tech infrastructure, users of technology and third parties.

24.4 Responsibilities

i. The Manager ICT shall be responsible for security and risk management of the entire ICT systems and the related infrastructure and shall report quarterly to management and the board.

ii. The PITO shall be responsible for implementing security controls and risk mitigation measures for IT systems and related infrastructure and thereafter training and sensitizing end users about the set controls and related trends from time to time.

iii. Pr. Comm Eng. shall be responsible for implementing security controls and risk mitigation measures for Telecom systems and the related infrastructure and thereafter training and sensitizing end users about the set controls and related trends from time to time.

iv. Pr. Ctrl Eng. shall be responsible for implementing security controls and risk mitigation measures for Power Control systems and related infrastructure and thereafter training and sensitizing end users about the set controls and related trends from time to time.

v. ICT system end users shall be liable, in their individual capacities, for abuse of security controls at their work stations

24.5 Procedure and Control

i. Access to ICT systems and Information shall be done through UserID and password and shall be granted only after approval by Manager ICT using ICT form 7.

ii. All data and information residing on ICT systems are private assets of UETCL and managed on a need to know basis.

iii. All data and information residing on ICT systems shall be protected in accordance with the Data Protection Act,

iv. Sensitive information shall not be kept on portable devices unless it is protected and/ encrypted.

v. Company information shall not be kept on portable devices unless it is protected and/ encrypted.

vi. All external connections shall be authenticated before access to information processing facilities is allowed.

vii. All internally and externally bound links to the network shall be compliant with standards relating to security and access controls including but not limited to filtering, logging, Virtual Private Network (VPN), two-factor authentication, WIFI passwords and encryption.

viii. Access rights to information residing on ICT systems including remote access for trouble shooting or support shall only be granted upon approval by the Manager ICT.

ix. Any component of the ICT system suspected of transmitting dangerous traffic shall be disconnected from the Local Area Network (LAN) immediately.

x. All servers and user workstations must be fitted with a fully licensed antivirus software and must be always kept up to date

xi. Users shall be provided with at least bi-annual security awareness and education about the impacts, preventative measures and actions against malicious code attacks

xii. Annual vulnerability assessments shall be conducted to identify potential weaknesses that could enable the introduction of malicious code.

xiii. Network security architecture shall be set up in such a way that it contains features to identify, record, alert and generate security audit reports.

xiv. Annually check and test restoration procedures to ensure their effectiveness and ascertain whether they can be completed within the time allotted in the ICT Disaster Recovery Plan (DRP).

xv. The following DRM controls shall be enforced;

- Use of USB ports shall be restricted unless authorized by MICT
- Flush disks authorized to move company data shall be password protected
- Firewalls shall be configured to restrict automatic forwarding of sensitive company data. Approval for any such forwarding shall be given by MICT
- All company laptop hard disks shall be encrypted

xvi. PITO, Pr. Com Eng and Pr. Ctrl Eng. shall design data loss prevention (DLP) measures and present them to MICT who will then present to the steering committee for buy-in and approval for implementation from time to time.

25 Business continuity Policy

25.1 The Policy

i. An ICT business continuity plan shall be implemented to limit interruption to business operations or where inevitable, re-establish normal business operations in a complete and timely manner in accordance with the ICT Disaster Recovery Plan (DRP).

25.2 Objectives

ii. Ensure that the ICT infrastructure has the capacity to withstand interruptions to critical business activities.

iii. To minimize the downtime and data loss in accordance with the DRP.

iv. Establish the criticality of different ICT facilities, systems, sites and networks by performing a business impact analysis of the unavailability of each ICT asset.

v. Ensure that continuity plans support correct information security levels.

vi. Ensure that appropriate continuity and recovery mechanisms are in place to meet or exceed the company wide business continuity targets.

vii. Ensure that the ICT infrastructure fulfils its ethical obligation to its internal and external stakeholders to protect and ensure continuity of UETCL business operations.

25.3 Scope

i. The ICT business continuity policy shall apply to all ICT facilities, systems, sites and networks.

25.4 Responsibility

i. MICT shall be responsible for the overall ICT business continuity plan design and execution. The role shall be played in consultation with the steering committee.

ii. PITO shall be responsible for the implementation, monitoring and testing of the ICT business continuity strategies for IT systems and related infrastructure.

iii. Pr. Com Eng. shall be responsible for the implementation, monitoring and testing of the ICT business continuity strategies for telecom systems and related infrastructure.

iv. Pr. Ctl Eng. shall be responsible for the implementation, monitoring and testing of the ICT business continuity strategies for Power Control systems and related infrastructure.

25.5 Procedure and Control

i. A disaster recovery and business continuity system shall be implemented in which data and applications stored on Storage Area Network (SAN) shall be replicated or backed up on a recovery site in a real-time manner.

ii. All business data within an employee's functional expertise shall be backed up regularly (in accordance with the DRP) and a record maintained in accordance with a backup strategy in the DRP.

iii. The contingency plan shall be tested annually, test results documented and reported to the ICT Steering Committee for review through MICT.

iv. The off-site backup and disaster recovery system shall be made active in the event of a disaster so as to ensure business continuity with minimum interruptions as stipulated in the DRP.

v. Critical business data shall be archived off site in accordance with the DRP and media stored in a secure and conducive environment.

vi. All users will store critical business data on the centralized storage media provided by the ICT department and not on local drives or any other personal media. It is the responsibility of the user to synchronize offline files in a timely manner upon reconnection to the network.

vii. Operations and maintenance department shall maintain a backup control Centre.

viii. Measures shall be put in place to ensure continuous power supply. These shall include but not limited to; Uninterrupted Power supply (UPS), generators, chargers and battery banks.

26 ICT Equipment Security Policy

26.1 The Policy

i. All ICT equipment shall be secured adequately using internal security and safety measures and controls in accordance with best industry standards and existing UETCL Insurance policy. Replacement of a lost un-insured ICT equipment without satisfactory explanation by the user will be done at a cost of the equipment book value to the user.

26.2 Objectives

i. To safe guard the ICT equipment from theft and or mysterious loss
ii. To enforce accountability and personal responsibility to those to whom ICT equipment has been allocated
iii. To protect and safeguard the data or information residing on the ICT equipment from leakage or illegitimate exposure upon disposal of the ICT equipment
iv. To enhance tracking of movement of ICT equipment
v. To ensure that the ICT equipment is used for authorized and legitimate purpose for which they were acquired.
vi. To ensure an auditable trail of disposal/destruction is evidenced.
vii. To provide advice on the appropriate methods of destruction of physical media

26.3 Scope

i. This policy applies to all ICT equipment purchased or leased by UETCL

26.4 Responsibilities

i. MICT shall be responsible for the overall security of ICT equipment save for SCADA equipment whose overall security shall be the responsibility of the Manager operations and Maintenance.
ii. PITO shall be responsible for the implementation of IT equipment security controls.
iii. Pr. Ctrl Eng. shall be responsible for the implementation of power system control equipment security controls.
iv. Pr. Com. Eng. shall be responsible for the implementation of telecom equipment security controls.
v. UETCL staff shall be personally liable and fully responsible for the security of the ICT equipment allocated to them.

26.5 Procedures and Control

ii. Allocations, movement and/ transfer of all ICT equipment shall be documented, approved and acknowled as described in form 1.

iii. A designated user of an ICT equipment shall be responsible for the security and safety of the subject ICT equipment.

iv. A designated user who will loose any un-insured ICT equipment without satisfactory explanation will be requred to pay the campany an amount to a tune of book value of equipment.

v. An up-to-date inventory of all ICT equipment shall be maintained by the ICT department using ICT form 4. A complete inventory of server room and IT network room equipment, including brands, models, serial numbers, and physical descriptions, should be completed and kept up to date.

vi. A logical and systematic naming convention shall be adopted to uniquely identify all ICT equipment and where applicable, shall match the corresponding asset tag.

vii. All critical ICT equipment shall be covered with adequate electronic insurance policy from a reputable Insurance company.

viii. A system for securely disposing of unwanted discs, tapes, cards, hard drives, printed paper, and anything else that could contain confidential information shall be implemented.

ix. Putting of UETCL ICT equipment to personal use at the expense of company work or any other such abuse is prohibited and punishable in line with the HR manual.

x. Disposal of ICT equipment shall follow the financial policies and procedure manual and the PPDA guidelines.

27 Bring Your Own Device (BYOD) Policy

27.1 The policy

i. Connectivity of any privately owned ICT devices on UETCL network shall be controlled. All non UETCL owned IT devices shall be granted access to UETCL network only through use of a duly approved ICT form 5.

27.2 Objectives

i. Establish guidelines for UETCL staff use of personally owned ICT equipment for official work related purposes.

ii. Protect the UETCL network from security attacks that may culminate from connections through BYOD devices.

iii. To safeguard staff against disruptions and interruptions in service that may occur on the ICT network due to BYOD

iv. To streamline the use of BYOD in UETCL by both internal and external stakeholders.

v. To allow staff secure access to business information and applications via devices that personally belong to staff for purposes of performing official duties.

27.3 Scope

i. This policy applies to all personal ICT devices that are capable of interacting with the UETCL ICT systems (Network and applications) including but not limited to; smart phones, tablets, laptops, GPS and desktops.

ii. The policy applies to both internal and external stakeholders.

27.4 Responsibilities

i. MICT shall be responsible for the overall BYOD control and risk management. This role shall be played in consultation with the steering committee.

ii. PITO shall be responsible for the implementation of BYOD controls, security and monitoring for the devices attaching to IT systems and related infrastructure.

iii. Pr. Com Eng. shall be responsible for implementation of BYOD controls, security and monitoring for the devices attaching to the UETCL Telecom network and related infrastructure.

iv. Pr. Ctl Eng. shall be responsible for implementation of BYOD controls, security and monitoring for the devices attaching to the UETCL power system control and related infrastructure.

v. Users of the authorized BYOD devices shall take full responsibility of their actions while operating these devices on the UETCL ICT network.

27.5 Procedures and Control

i. Request for connectivity and use of own ICT device shall be done on ICT Form 5 by the requester and approved.

ii. The number of privately owned ICT devices connected on UETCL network shall be limited to only two (2) per person.

iii. Accessibility and use of private owned ICT devices shall be guided by the ICT Systems and Information security policy and Guidelines.

iv. Connectivity of a privately owned device shall be granted for only a specific period of time.

v. BYOD devices must be presented to the responsible officers (PITO for IT, Pr. Ctrl Eng. for Power control systems and Pr. Com Eng for telecom systems) for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

vi. In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the company network.

vii. The UETCL strong password policy is as described in the password policy in this manual

viii. The device must lock itself with a password or PIN if it's idle for at least five minutes.

ix. Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the ICT network.

x. Employees' access to company data via BYOD shall be limited based on user profiles defined by ICT and automatically enforced. Such controls shall include but not limited to encryption, automatic log-out after 5 minutes of inactivity and automatic lock-out after three unsuccessful log-in attempts.

xi. The employee's device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

xii. The company reserves the right to disconnect devices or disable services without notification.

xiii. The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.

xiv. The employee is personally liable for all costs associated with his or her device save for internet data costs where the company may provide as and when deemed fit.

xv. The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

xvi. The BYOD devices shall be used in accordance with the acceptable use policy in this policy manual.

28 User Support Policy

28.1 The Policy

i. The ICT department shall provide reliable internal technical support to the satisfaction of in-house ICT system users and any other stakeholders. Technical user support for specialised software applications and infrastructure systems shall be outsourced from the original authors, manufacturers or authorised service providers. The ICT user support policy shall be executed in tandem with the ICT service level agreement between the ICT department and the users.

28.2 Objectives

i. To ensure continuity of ICT services with minimal interference

ii. To streamline the ICT – User relationship by setting standards for ICT service delivery and managing expectations from either parties.

iii. To describe the basic level of service that will be guaranteed by the ICT department to UETCL employees.

iv. To identify and delineate the limits of ICT’s capabilities and what will not be supported.

v. To ensure ICT facilities are put to maximum use as per objective of their acquisition and in line with the overall company strategy and objectives.

28.3 Scope

i. This policy will apply to all UETCL owned ICT applications and devices.

28.4 Responsibilities

i. MICT shall be responsible for the overall ICT user support management

ii. MICT shall be responsible for ensuring that ICT support personnel are provided with all the necessary work tools, safety gear and training.

iii. PITO shall be responsible for collecting and responding to IT user support requirements in accordance with the underlying ICT service level agreement

iv. Pr. Com Eng. shall be responsible for collecting and responding to telecom user support requirements in accordance with the underlying ICT service level agreement

v. Pr. Ctl Eng. shall be responsible for collecting and responding to Power systems control user support requirements.

vi. ICT users shall be responsible for reporting collectively or individually their ICT support requirements to the responsible officers as stipulated in this policy document and the ICT service level agreement.

28.5 Procedures and Control

i. User support shall be guided mainly by the ICT Service Level Agreement.

ii. User support shall be managed through an automated help desk using a well-managed user support tool through which staff shall report system issues requiring support.

iii. Highly specialised applications and systems shall be supported through a service level agreement with the system suppliers, authors or their local representatives.

iv. All network devices including any data traffic shall be monitored using firewalls in order to detect and respond to faults immediately and ensure network security.

v. Modification of any network connections shall only be done by ICT support staff.

vi. All users shall guard against any abuse that may disrupt or threaten the availability of all ICT systems.

vii. PITO shall ensure that installation and configuration of all hardware and software is aligned to approved ICT standards

viii. PITO shall ensure that all IT support Desk activities are recorded and updated in the Help Desk Job Register; ensures all help desk problems causing support resolution delays are documented and reported

ix. PITO shall coordinate with external support escalation entities relating to User hardware and locally installed software. i.e. ensure support is provided for both on-site and from externally-based support.

29 ICT Infrastructure maintenance policy

29.1 The Policy

i. All ICT infrastructure and related peripherals shall be maintained in good working condition in accordance with regulatory requirements, industry best practices and as recommended by the manufacturers.

29.2 Objectives

ii. To maintain at least 98% annual infrastructure availability levels

iii. To ensure ICT infrastructure returns the value and benefits for which it was installed in accordance with the company objectives.

iv. To enforce compliance to maintenance best practice for the safety of the infrastructure

v. To document maintenance routines and schedules

vi. To effectively, efficiently, economically and sustainably utilise the current and emerging infrastructure needs of UETCL.

vii. To ensure timely capacity requirement identification through continous monitoring and tuning.

29.3 Scope

This policy shall cover all ICT hardware devices such as network devices, optic fibre links, telecom interfaces, servers (SCADA, IT and telecom), workstations, laptop, storage, back-up, operating facilities and supporting platform like operating systems and databases.

29.4 Responsibilities

i. MICT shall be responsible for the overall maintenance of the ICT infrastructure

ii. PITO shall be responsible for collecting and responding to IT infrastructure capacity and maintenance requirements in accordance with the underlying ICT service level agreement

iii. Pr. Com Eng. shall be responsible for collecting and responding to telecom infrastructure capacity and maintenance requirements in accordance with the underlying ICT service level agreement

iv. Pr. Ctl Eng. shall be responsible for collecting and responding to Power systems control capacity and infrastructure maintenance requirements.

v. ICT users shall be responsible for reporting collectively or individually their ICT capacity and infrastructure support requirements to the responsible officers as stipulated in this policy document and the ICT service level agreement.

29.5 Procedures and control

i. The ICT department shall be responsible for maintenance of all mainstream ICT infrastructure and related peripherals, including managing capacity and any outsourced contract(s).

ii. SCADA related infrastrcuture shall be maintained by the Operations and Maintenance department including capacity management

iii. Services or tasks for which the internal capacity is insufficient shall be outsourced.

iv. All ICT infrastructure shall be kept in conducive and favourable environments.

v. A maintenance schedule shall be developed and a log sheet maintained for each of the infrastructure equipment.

vi. The ICT department shall conduct periodic inspections each calender year for senstive ICT infrastructure such as battery banks, Battery Chargers, Servers, PCs, PLCs, etc and compile health status and capacity reports on their conditions.

vii. All obsolete ICT equipment will be declared to Finance, Accounts and Sales department so as to update the asset register accordingly.

viii. All capacity requirements shall be collected and responded to by the responsible officers above in maner as to avoid service outage for services critical to the UETCL business.

ix. PITO, Pr.Com Eng and Pr. Ctrl Eng shall be equiped with tools to detect capacity deficiency to be reported and action taken before exceeding 70% of the full capacity for any infrastructure component including hard disks, memory, processors, data points etc.

x. The ICT department shall maintain a clear and up-to-date ICT system topology with a standard nomenclature of all ICT infrastructure and infrastructure organisation.

30 ICT Hardware useful life policy

30.1 The Policy

i. Various ICT equipment will be due for replacement due to wear and tear after being used for the respective years indicated against each of the equipment in table 1 and table 2 below. Any equipment declared unusable will be documented and approval will be sought from the ICT steering committee to have it disposed off following the set PPDA disposal procedures.

30.2 Objectives

i. To enforce usage of equipment for only the period within which it is deemed technically useful by the manufacturer and by experience and best practice

ii. To provide guidelines regarding when ICT equipment is due for disposal and or replacement.

iii. To clearly stipulate the expected useful life for each major ICT equipment

iv. To provide guidelines for cleaning up the ICT equipment fleet by scrapping and restocking in a timely manner.

v. To protect human health and the environment

vi. To protect sensitive data from leakage upon disposal

30.3 Scope

i. This policy shall cover all ICT equipment that are categorized by the Financial policies and procedure manual as assets.

30.4 Responsibilities

i. MICT shall be responsible for the entire management of equipment useful life.

ii. PITO shall be responsible for monitoring, identifying and collecting IT equipment at end of useful life

iii. Pr. Com Eng. shall be responsible for monitoring, identifying and collecting telecom equipment at end of useful life

iv. Pr. Ctl. Eng. shall be responsible for monitoring, identifying and collecting Power systems control equipment at end of useful life.

v. ICT users shall be responsible for reporting collectively or individually their ICT equipment health status to the above responsible officers for diagnosis and respective technical assessment

vi. MICT shall work in conjunction with the Head of department responsible for SHE matters to ensure that a complete sanitization process of storage media is adhered to upon disposal in accordance with the UETCL SHE policy.

30.5 Procedures and control

i. The first fundamental step shall be identification and collection of the equipment that has hit end of useful life by the responsible officer and presented for assessment

ii. An assessment shall be done to ascertain whether the equipment can or cannot serve the intended user or has been in operation for the specified number of years to qualify it for end of life in accordance to this manual.

iii. An up to date ICT inventory database shall be maintained by each responsible officer in their areas of jurisdiction (Telecom, IT and power systems control).

iv. Equipment shall be categorised as capital or non-capital equipment following the guidelines in the FPPM

v. The useful life for key ICT equipment shall follow the durations prescribed in the table below;

Table 1: IT equipment with their respective years of useful life

No	ICT Equipment	Years of Useful life
1	Storage Area Network (SAN)	10
2	Servers	5
3	Workstations	5
4	Personal Computers	3
5	Laptops, Tablets and IPADs	3
6	Printers	3
7	Access control devices	5
8	CCTV equipment (Cameras, DVRs, etc)	3
9	Switches	5
10	Routers	5
11	Projectors	3
12	Photocopiers	3

Table 2: Communication equipment with their respective years of useful life

No	ICT Equipment	Years of Useful life
1	Battery banks (Alkaline)	10
2	Battery Banks (Lead Acid)	5
3	Battery Charger (Switched Mode)	7
4	Battery Charger (Thyristor controlled)	10
5	Standby Generators	7
6	Power Line Carrier (PLC)	7
7	Universal Multiplexers (UMUX)	7
8	Flexible Multiplexer (FMX)	7

No	ICT Equipment	Years of Useful life
9	Megaplex	7
10	HIT 7025	7
11	Mobile Phones and PDAs	2
12	VOIP desk Phones	3
13	VOIP Communication Server	5

31 CCTV Policy

31.1 The Policy

i. UETCL shall use Close Circuit Television ("CCTV") within some of its premises including offices, plant houses, substations and POPs. The purppose of the policy is to set out guidelines on the management, operation and use of the CCTV across the UETCL premises.

31.2 Objectives

UETCL shall use CCTV for the following purposes;

ii. Deter crime on UETCL premises
iii. Monitor operational activities at the different sites including substations fiber POP houses
iv. Provide evidence during investigations
v. Keep a record of the footage at the different sites where they (CCTV) cameras have been deployed.
vi. Real time surveillance
vii. To provide a safe and secure environment for its staff, visitors and stakeholders
viii. To prevent the loss of or damage to the UETCL facilities and/or assets
ix. To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders

31.3 Scope

i. This policy applies to all members of UETCL workforce, visitors, stakeholders and all other persons whose images may be captured by the CCTV system.

31.4 Responsibilities

ii. The Principal security officer shall be in charge of the real time monitoring of CCTV footage with the aim of taking proactive action on any perpetrator caught in action real time
iii. The PITO shall be responsible for the technical setup, maintenance and support of the CCTV installation aiming at least 95% availability
iv. PITO shall be in charge of backup and playback of CCTV footage on request

v. MICT shall play the overall oversight role for the functionality of the CCTV platform

vi. MCS shall play the overall liaison role between ICT and security to enforce efficiency of CCTV performance and ensure the intended objectives of the installations are achieved.

31.5 Responsibilities and Control

31.5.1 Siting of Cameras

i. All CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff, stakeholders and visitors.

ii. Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. UETCL (ICT) shall make all reasonable efforts to ensure that areas outside of UETCL premises and grounds are not recorded.

iii. Signs shall be erected to inform individuals that they are in an area within which CCTV is in operation.

iv. Cameras Shall not be sited in areas where individuals have a heightened expectation of privacy, such as open offices area, closed offices or toilets.

v. Cameras may be located in open offices where this is the case, employees, stakeholders and visitors shall be made aware. Access to the footage is restricted and shall only be used to fulfil the purposes in 23.2

31.5.2 Privacy Impact Assessment

i. Prior to the installation or repositioning of any CCTV camera, or system, a privacy impact assessment shall be conducted by the UETCL (ICT and Security committee) to ensure that the proposed installation is compliant with prevailing legislation where applicable. The assessment will be approved by the ICT and security Committee.

ii. ICT shall adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.

iii. The CCTV system in UETCL shall be managed by a member of the ICT Department.

iv. Any allegations against UETCL staff shall be referred immediately to the Principal Security Officer and only he shall determine who needs to view the footage. Allegations against the principal security officer and his team will be referred to the Chief Executive Officer (CEO). Allegations management staff will be referred to the CEO. Allegations against the CEO will be referred to the Chair of the Board

v. On a day to day basis the CCTV system will be operated by an individual with appropriate technical ability in the CCTV systems domain.6.4 The viewing of live CCTV images (observation centre) will be restricted to the ICT and Security management team and others delegated by the UETCL Senior Management Team. In doing so they will ensure that, the purposes in 2.1 are satisfied.

vi. Recorded images, which are stored by the CCTV system, will be restricted as in 6.4. Relevant images may be shared with governing body panels reviewing exclusions, disciplinary matters or complaints.

vii. No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to disclosure of images.

viii. The CCTV system is checked daily to ensure that it is operating effectively by the Security team or its agents and must report to the ICT team immediately if there is an anomaly.

31.5.3 Storage and Retention of Images

i. Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded.
ii. Recorded images are stored for a maximum of 13 days unless there is a specific purpose for which they are retained for a longer period.
iii. ICT team will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:
iv. CCTV recording systems being located in restricted access areas;
    a) The CCTV system being encrypted/password protected;
    b) Restriction of the ability to make copies to specified members of staff
    c) A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images, will be maintained by the ICT team.

31.5.4 Disclosure of Images to Data Subjects

i. Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation, and has a right to request access to those images.
ii. Any individual who requests access to images of themselves shall be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be considered in the context of the UETCL's Access Request Policy.
iii. When such a request is made the appropriate individual with access to the CCTV footage (ref 6.4) shall review the CCTV footage, in respect of relevant time periods where appropriate, If the footage contains only the individual making the request then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The individual accessing the footage must take appropriate measures to ensure that the footage is restricted in this way.

iv. If the footage contains images of other individuals, then the ICT and Security management committee must consider whether:

a) The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other

b) If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

v. A record must be kept, and held securely, of all disclosures, which sets out:

a) When the request was made;

b) The process followed by to the individual with access to the CCTV footage in determining whether the images contained third parties;

c) The considerations as to whether to allow access to those images;

d) The individuals that were permitted to view the images and when; and

e) Whether a copy of the images was provided, and if so to whom, when and in what format.

***Note** that, when an access request is made then, unless an exemption applies (such as in relation to third party data that it would be unreasonable to disclose) then the requester is entitled to a copy in a permanent form. There is reference here only to "access" as opposed to a "permanent copy" as the UETCL may consider it preferable in certain circumstances to seek to allow access to images by viewing in the first instance without providing copies of images. If an individual agrees to viewing the images only then a permanent copy does not need to be provided. However, if a permanent copy is requested then this should be provided unless to do so is not possible or would involve disproportionate effort*

31.5.5 Disclosure of Images to Third Parties

i. The UETCL/Trust will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection and privacy Legislation.

ii. CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.

iii. If a request is received from a law enforcement agency for disclosure of CCTV images, then the individual with access to the CCTV footage must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third party images.

iv. The information above must be recorded in relation to any disclosure.

v. If an order is granted by a Court for disclosure of CCTV images, then this should be complied with. However very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure, then the Data Protection Officer or equivalent should be contacted in the first instance and appropriate legal advice may be required.

32 ICT Architecture Management policy

The policy provides an understanding of all the different elements that make up UETCL and how these elements interrelate, enabling the organization to effectively achieve its current and future objectives. ICT architecture design shall act as an interface between ICT designers and planners, UETCL business strategist, designers, and planners. The ICT architecture design shall draw the line about what can be done or cannot be done from ICT point of view.

32.1 Objectives

i. To balance between innovation, risks, and costs.
ii. To provide a basis for the analysis of an ICT service behaviour before the service has been built.
iii. To allow the ICT team to verify that the service being designed will fulfil all the stakeholders' needs
iv. To save costs when updates to existing ICT services or new services with many commonalities with existing services are designed in the future.
v. ICT architecture **facilitates the communication between** stakeholders in order to deliver a system that fulfils their needs. i.e. stakeholders need to understand the technical consequences of their needs.

32.2 Scope

i. The policy shall cover; IT, communication and control systems architecture including design needs in areas of infrastructure, equipment, data, application, and external stakeholder services.

32.3 Responsibilities

ii. Manager ICT shall be responsible for the overall ICT architecture

iii. P. Ctrl. Eng. Shall be responsible for the design and implementation of the power system architecture.

iv. PITO shall be responsible for the design and implementation of the IT systems architecture.

v. P. Com. Eng. Shall be responsible for the design and implementation of the communication systems architecture.

32.4 Procedures and control

i. Changes to applications and technology shall only be made in response to business needs.

ii. Technological diversity shall be controlled to minimise the non-trivial cost of maintaining expertise in and connectivity between multiple processing environments.

iii. Software and hardware shall always conform to the defined standards that promote interoperability for data, applications and technology.

iv. Integration with existing on-premises and other cloud services shall be considered in the enterprise architecture. This shall be done in consultation with the steering committee.

v. Before contracting with a Cloud Computing provider, assurance shall be ascertained about the level of Information Security provided.

vi. The ICT enterprise architecture shall be reviewed every five years to ensure Effective Enterprise Architecture is achieved through the application of a comprehensive and thorough process for describing a current and future structure and behaviour for the UETCL processes, Information, applications, technology and supporting human resources.

33 Tele Commuting policy

33.1 The policy

i. UETCL considers telecommuting to be a viable alternative work arrangement in cases where individual, job and supervisor characteristics are best suited to such an arrangement. Telecommuting allows an employee to work at home, on the road, or in a satellite location for all or part of their regular workweek supported by technology.

33.2 Scope

i. The policy applies only to employees who have been authorized by the Chief Executive Officer or Manager Human Resource and Administration.

33.3 Objectives

i. To fulfil specific operational needs especially during difficult situations such as the COVID-19 pandemic situation or as part of a disaster recovery or emergency plan or such as may be authorized by MHR&A and the steering committee or any other relevant task force so created from time to time.

ii. To streamline guidelines on how to facilitate staff authorized to work remotely

iii. To enable operational continuity even during times of constraint for workers' physical presence at their designated work stations.

33.4 Responsibilities

i. Manager ICT shall be responsible for the overall coordination of the ICT telecommuting requirements. This role shall be played in consultation with the steering committee.

ii. P. Ctrl. Eng. Shall be responsible for the design and implementation of the power system related telecommuting requirements.

iii. PITO shall be responsible for the design and implementation of the IT systems related telecommuting requirements.

iv. P. Com. Eng. Shall be responsible for the design and implementation of the communication systems related telecommuting requirements.

33.5 Procedures and Control

i. Employees ("Telecommuters") who are authorized to perform work at off-site work locations must meet the same standards and professionalism expected of UETCL employees at onsite work locations in terms of job responsibilities and work products.

ii. Telecommuters shall be facilitated with the following ICT requirements (at least);

   a. Laptop
   b. Internet
   c. Remote access to the UETCL LAN

iii. The Telecommuters must establish an appropriate environment within their home for work purposes to ensure limited interruption and safety of the ICT equipment.

iv. UETCL shall reimburse the employee for business-related expenses such as long-distance phone calls and internet data that are reasonably incurred in accordance with job responsibilities and claimed through UETCL standard reimbursement policy and procedures.

v. Consistent with expectations of information asset security, telecommuting and remote working employees will be expected to ensure the protection of vital company information accessible from their home office. Security steps include, but are not limited to: 1. Use of locked file cabinets and desks; 2. Regular password maintenance; 3. Any other steps appropriate for the job and the environment.

34 Telephony

34.1 Policy

i. UETCL shall provide staff with telephone services including desk phone and/or mobile phones as deemed appropriate to facilitate business operations and communication.

34.2 Objectives

i. To ensure reliable and uninterrupted voice communication between staff members and stake holders within and outside the UETCL administrative offices and substations.

ii. To ensure and/ or boost operational and administrative effeciency

iii. To ensure continous availability of the communication service to promote safe operations.

34.3 Scope

iv. The fixed base phone network located in all UETCL administrative offices and substations.

i. The mobile Closed User Group (CUG) and other corporate mobile phone services

ii. This policy also covers the VHF communication.

34.4 Responsibility

i. MICT shall be responsible for the overall telephone and voice infrastructure.

ii. It shall be the responsibility of the PCE to ensure that the telephone network is operational with an uptime or availability of 99.999%

iii. It shall be the responsibility of the Pr. Com. Eng. to ensure that the PSTN with the widest coverage and optimal cost is chosen to offer the CUG service in order to ensure value for money.

iv. PCE shall be reponsible for the regstration of all CUG SIM cards in the names of UETCL.

v. It shall be the responsibility of the Pr. Com. Eng. to plan, design, implement, monitor and maintain the telephone network.

vi. It shall be the responsibility of PITO to ensure availability of the underlying IT infrastructure upon which the telepnone service is delivered.

vii. Users shall be responsible for the acceptable usage, safety and good care of the telephone devices allocated to them including timely reporting of damage or loss.

viii. Use of the CUG shall be mandatory unless otherwise declared faulty

34.5 Procedures and Controls

i. The Pr. Com Eng. shall install and maintain an up to date telephone network in all UETCL administrative offices and substation, implying updated directory, coverage, technology and documentation.

ii. Where ever technically possible (presence of the corporate LAN and structured cabling infrastructure), the UETCL telephone network shall be based on the Internet Protocol (VoIP)

iii. For redundancy, the UETCL telephone network shall consist of more than one exchange (communication server) installed at different locations.

iv. The telephone network shall be secure and centrally managed by a robust and reliable management system.

v. There shall be coordination between the IT network administrators and the telecom engineers whenever LAN system upgrades, scheduled maintenance or major changes are to take place in order to avoid disruption to the VoIP network.

vi. In conjunction/partnership with a PSTN, UETCL shall offer mobile CUG services to its staff (including the mobile handset). The PSTN chosen shall have coverage in all UETCL areas of operation (including transmission lines and substations).

vii. For survivability and redundancy, there shall always be more than one PSTN connection. These connections shall be interfaced to different switches.

34.5.1 VoIP User Management

i. Pr. Com Eng. shall maintain an updated phone directory including both fixed desk and mobile phone numbers. New users shall be created after the approval of the MICT and deleted upon the termination of their contracts with UETCL.

ii. Users shall be managed through a centralized management system by granting and removing various privileges as and when instructed by MICT through the Pr. Com. Eng.

iii. There shall be continuous monitoring and reporting of the telephone network and its usage.

iv. Management reserves the right to record telephone users for operational, administrative or security reasons.
v. All power system control related telephone calls shall always be recorded.

34.5.2 CUG Enrolment

i. Pr. Com. Eng. shall ensure that all CUG sim cards are duly registered in the names of UETCL
ii. Pr. Com. Eng. shall manage the CUG contract on behalf of UETCL to ensure that the PSTN adheres to the provisions of the contract
iii. Upon recruitment, the new staff member shall be allocated a new CUG SIM card and a mobile phone handset not later than 20 working days after confirmation and acceptance of the UETCL offer.
iv. Upon termination of employment, staff shall handover the CUG device with its SIM card in accordance with the HR manual provisions.

34.5.3 Call Budget Management

i. The telephone system shall be configured in such a way as to utilize the least cost route for outgoing calls.
ii. The call costs for all staff specifically the outgoing calls shall be managed and budgeted for by the Pr. Com. Eng in coordination with the MICT.
iii. MICT shall allocate, to the approved members of staff, a monthly budget for telephone calls in accordance with the approved ERA annual telephone budget.
iv. The issuance and usage of the allowance shall be transparent and accessible to the individual members of staff.

35 Optical Fiber

35.1 Policy

i. UETCL shall maintain a fiber network that conforms to the ITU-T G series and FOA standards for business communication. The excess cores of the fiber will be leased out for revenue generation purposes.

35.2 Objective

i. The availability of the optical fiber shall not be less than 99.8%
ii. To provide reliable and redundant optical fiber links for UETCL services and clients.

35.3 Scope

The entire UETCL optical fiber network including the following:

- OPGW, ADSS & SKYWRAP fiber installed on the transmission grid (66KV, 132KV, 220KV & 400KV transmission lines)
- ADSS fiber installed on the distribution (33KV & 11KV) grid for UETCL
- Underground fiber installed for UETCL

35.4 Responsibility

i. MICT shall ensure that the Communication section is adequately staffed and equipped to maintain the optical fiber network. MICT shall also manage communication with internal and external stakeholders.

ii. PCE shall ensure that there is sufficient budget to gradually build a reliable and redundant fiber network.

iii. PCE shall also ensure the timely corrective action in case of any emergency breakdowns/failures

iv. PCE shall ensure sufficient stock levels (at least 10%) of spares for recovery from any unscheduled disaster.

v. The PCE shall ensure that there are adequate and sufficient tools to carry out all maintenance works on the optical fiber network.

35.5 Procedures and Controls

35.5.1 General guidelines for optical fiber cable Indoor & outdoor Installation

The guidelines that shall be applied during cable installations are as follows:

i. A thorough site survey shall be conducted prior to the cable placement

ii. A cable pulling plan shall be developed.

iii. For premises installation, all cable installations shall meet building and fire codes. Also, all penetrations of fire-rated walls shall be fire stopped.

iv. Cable minimum bend radius and tension shall not be exceeded.

v. Cable maximum recommended load shall not be exceeded

vi. The installation shall be documented

35.5.2 Preventive Maintenance

The following shall be taken into consideration:

i. Well trained and certified personnel shall be employed. Alternatively, the existing staff shall be empowered and certified with appropriate skills
ii. The maintenance teams shall have up to date and well calibrated tools and equipment.

The steps below shall be taken to forestall future failures

i. Patrol and Inspection – To look out for the following:
   a. Cable route conditions
   b. Condition of the cable, splice canisters, cable loops and connectors (for indoor or external ODF applications).
   c. Relative distance between the cable and third party activities (like construction)
   d. Damage to the infrastructure due to natural conditions, such as floods, lightening, etc.
   e. Damage to the infrastructure due to other projects, such as construction of roads, pipelines, and buildings.
   f. Damage to the infrastructure due to vandalism and theft.
   g. Damage to the infrastructure due to attack by other creatures e.g. rodent, birds (woodpecker) etc.
ii. Periodic Cable Test – Spare optical fibres shall be tested at the ODF (Optical Distribution Frame/FDF (Fiber Distribution Frame). Remote Fiber Monitoring Systems (RFTS) shall be deployed to continuously monitor the performance of the fiber, locate faults precisely (issuing GPS coordinates) and document the fiber plant as required by the regulator.
iii. The cable plant shall be precisely documented and well labelled (at commissioning and after any changes or additions) as it makes trouble shooting and restoration much faster

35.5.3 Corrective Maintenance

i. Upon breakage of the fiber cable the very first step shall be fault localization. This shall be done fast in order to reduce to down time.
ii. The RFTS shall automatically and precisely detect the location of the breakages and degradation.

iii. The MICT & PCE shall be informed immediately of the breakage or significant degradation so that they can manage the communication with both internal and external stakeholders and also approve release of resources (personnel, tools and allowances).

iv. A work order shall be issued and a repair team immediately dispatched. The following steps shall be implemented:

  a) A temporary fiber replacement route shall be provided where possible.
  b) The number of personnel required shall be determined and mobilized.
  c) The necessary tools, test instruments, and materials shall be prepared and transported to the fault location.
  d) The ADMs at both ends of the link shall be disconnected (if without ALS & ALR)
  e) The fiber cable shall then be repaired or replaced.
  f) For efficient maintenance of the optic fiber cable, motor vehicles shall be provided and maintained ready for use at all times.
  g) A sufficient force of men trained in fiber cable maintenance shall be kept within reasonable travelling times.

35.6 Commercialization of the fiber

UETCL shall obtain requisite license to enable it lease out the following services:

i. Dark fiber cores
ii. Telecom Capacity
iii. Colocation

The following steps shall be followed by any potential client:

i. Formally write to the Manager ICT expressing interest in a specific service(s)
ii. The Manager ICT shall engage the potential client and present the options available and indicative prices
iii. If still interested, the potential client will have the option to carry out a site survey of the infrastructure and if required, a test can be carried out to prove

the capabilities of the UETCL infrastructure. In any case, the test shall not take more than one week

iv. If still interested, the contract between UETCL and the potential client will then be drawn up, reviewed by both sides and signed. The contract will also include a Service Level Agreement (SLA) and Escalation Matrix (templates for both attached in the appendix)

v. After having completed all legal requirements of the contract, the client will then proceed to install their equipment in the UETCL premises/substations under the supervision of the UETCL technical personnel.

35.6.1 Access to UETCL Sites

The client shall access the UETCL sites under the following circumstances:

35.6.2 Scheduled Maintenance Activities

Whenever the client would like to access their equipment for scheduled maintenance activities, they shall send an email to the Principal Communication Engineer at least three (3) days prior to the activity. The template for the access form is attached in the appendix

35.6.3 Emergency Maintenance Activities

Emergency access applies whenever there is a traffic affecting condition/fault on the clients' equipment. In this case, the client should write/email the Principal Communication Engineer immediately and access will be granted in no less than thirty minutes. The template for the access form is attached in the appendix

36 ICT Infrastructure Maintenance

36.1 Policy

i. All ICT infrastructure and related peripherals shall be maintained in good working condition in accordance with regulatory requirements, industry best practices and as recommended by the manufacturers.

36.2 Objective

iii. Ensure that the equipment lives out its entire expected lifespan.

iv. Ensure that the equipment availability is maintained at 99% through a robust maintenance schedule and ensuring redundancy in the core equipment (especially the auxiliary power supplies)

v. Ensure that adequate budgets are available to carry out the maintenance activities

36.3 Scope

This policy applies to all ICT equipment as shown in the table 1 & 2 above:

36.4 Responsibility

vi. PCE shall ensure that the scheduled equipment maintenance for the Telecommunication and Auxiliary Supplies is carried out in a timely manner and all required resources availed to the technical personnel

vii. PCE shall ensure the timely repair/replacement of any emergency breakdowns/failures

viii. PCE shall ensure that the stock levels for any vital spares of the telecommunication equipment and auxiliary supplies is maintained at 10%

ix. PITO shall ensure that the scheduled equipment maintenance for the IT equipment is carried out timely and all required resources availed to the technical personnel

x. PITO shall ensure the timely repair/replacement of any emergency breakdowns/failures

xi. PITO shall ensure that the stock levels for any vital spares of the IT equipment is maintained at 10%

36.5 Procedures and Controls

36.5.1 Maintenance of Battery Banks

For safety reasons, the following shall be available: Googles, Face shield, Gloves, Apron, Eye wash, a source of running water

Scheduled maintenance shall be carried out biannually and a detailed report submitted to the PCE. The following steps shall be taken:

i. Visual inspections (under normal float conditions) to determine the following:
   a. Intact cell vent plugs
   b. Intact plastic containers (no leakage of electrolyte)
   c. Intact terminals (positive & negative, no salt accumulation)
   d. Intact connectors (no hot spots & loose connectors)
   e. Intact terminals & connectors (no evidence of corrosion)
   f. Intact battery racks (no evidence of corrosion)
   g. Intact cell electrolyte level (between MIN & MAX level mark)
   h. Intact battery, clean & dry (free from dust and damp)
   i. Intact battery room ventilation

ii. The cell voltages along with the cell number shall be recorded along with the terminal voltage, float current and temperature.

iii. A float charge test shall then be carried out and the charging voltage, current and battery voltage noted down.

iv. Corrective action shall be taken. In case of water replenishment, the quantity should be noted.

v. Discharge test of the battery bank up to the minimum system voltage (according to the instructions of the manufacturer) shall be carried out. The cell voltages, discharge current and discharge time shall all be periodically (preferable hourly) noted.

vi. A high rate charge test shall also be carried out (according to the instructions of the manufacturer) to charge the batteries back to float level. The charging current, voltage and time shall be noted.

36.5.2 Maintenance of Battery Chargers

Scheduled maintenance shall be carried out biannually and a detailed report submitted to the PCE. The following shall be checked:

i. The floating voltage (normal operating) - To ensure that it is within the allowable range (refer to the charger and battery manufacturer for the appropriate range). If not, shall be adjusted accordingly.

ii. The boost voltage (quick charge operating) – To ensure that it is within the allowable range (refer to the charger and battery manufacturer for the appropriate range). If not, shall be adjusted accordingly.

iii. Mechanical parts (e.g. screws) should be checked, to ensure that they are still rightly fixed.

iv. The air inlet and outlet shall be cleaned. Dust shall be removed by suction. Compressed air shall not be used, as dust particles may enter the interior of the rectifier part.

v. It is recommended that the rectifier bridge fan and chemical capacitors (if possible) be replaced every five years.

36.5.3 Maintenance of Standby Generators

Scheduled maintenance shall be carried out quarterly and a detailed report submitted to the PCE. The following shall be checked:

i. **Visual Inspection** – The surrounding area shall be free of debris and well ventilated. The inspection shall be done when the generator is not running. One should look out for the following:

   a) Oil and coolant shall not be leaking.

   b) The exhaust system including the manifold, muffler and exhaust pipe shall not have leakages.

   c) Connecting gaskets, joints and welds shall be checked for leakages.

   d) Connections shall be tight and free from corrosion.

   e) The starting and electrical system shall be clean.

   f) Ant adverse conditions shall be corrected promptly by qualified technician.

ii. **Cooling system:**

a) The coolant used shall be approved by the manufacturer for the engine.
b) The coolant level shall be checked.
c) The radiator shall be free from dust and debris.
d) The coolant heater shall be checked.

iii. Fuel System:

a) The fuel shall be checked as well to ensure that it has not degraded. Samples shall be taken from the fuel supply lines and the bottom of the tank. The fuel shall be filtered or changed if not satisfactory
b) Fuel tanks shall be sized so that the fuel is turned over on a regular basis
c) Charge air piping, supply hoses shall be examined for leaks. One shall also look out for damaged seals as well.
d) The fuel delivery system should be examined for leaks and correct pressure.

iv. Batteries and Wiring:

a) The battery shall be kept clean and free from corrosion
b) The battery voltage, specific gravity and electrolyte levels shall also be checked
c) The terminals on the battery shall be tight and the battery should be fully charged.
d) The operation of the battery charger (trickle charger) shall be verified.
e) Both the battery and the trickle charger shall be checked at least monthly

v. Generator exercise:

a) The generator shall be exercised monthly with at least 30% of the rated capacity for a minimum of 30 minutes.
b) The generator shall be exercised for at least one hour at 100% of rated capacity for at least once a year. A load bank shall be used if not possible to use a site load.
c) Testing shall be done through the ATS to ensure the entire system works properly.

vi. A framework contract for maintenance of the generators shall be signed with a competent contractor to ensure that service is carried out in a timely manner and also drastically reduce the down time during emergency breakdowns

vii. The scheduled/preventive maintenance of the generator should be done quarterly or after 250 hours (whichever comes first)

36.5.4 Maintenance Procedures for the Multiplexers

36.5.4.1.1 Maintenance Precautions

i. **Board Maintenance**

   a. Proper antistatic measures like wrist straps shall be worn
   b. Attention shall be paid to the damp-proof handling of the boards to prevent moisture from condensing on the board.
   c. Care shall be taken when plugging and unplugging boards in order not to damage the pins that connect to the mother board

ii. **Optical Interface Maintenance**

   a. The optical interfaces of the optical interface board shall always be covered with dustproof caps
   b. The fiber pigtail connectors shall always be covered with dust caps once unplugged
   c. One shall never look straight into the optical interface on the optical board
   d. Dust-free paper dipped in absolute alcohol shall be used to carefully clean the fiber pigtail connectors. Ordinary industrial alcohol, medical alcohol, and water shall not be used.
   e. Fiber pigtails on the optical board shall be unplugged before replacing an optical board.

iii. **Equipment maintenance**

   a. Power cables shall never be installed or disconnected without turning off the power switch
   b. The cabinet door shall always be closed to ensure the equipment always has an excellent anti electromagnetic-interference performance.

iv. **EMS/NMS Maintenance**

   a. The EMS shall always be on and operating to ensure the continuity of equipment monitoring.
   b. Different EMS login accounts for different users with different authority shall be assigned. The passwords shall be periodically changed
   c. Data shall be periodically backed up to ensure quick recovery in case of a fault.

36.5.4.1.2 Maintenance Operations

The routine maintenance shall be carried out quarterly, well documented, and the and the issues below observed:

a) confirmation that the Audio alarms (if available) are operational. A simulation of the alarm shall as well be done to confirm.

b) Cabinet Indicators – Checking the status of the indicators on the top of the cabinet

   i. If any, the cause of the alarm shall be ascertained and cleared.

c) **Board Indicators** – Checking the status of the indicator lights of the board.

   i. If any, the cause of the alarm shall be ascertained (either using the LCT or the EMS) and cleared

d) **The Fan** – Good heat dissipation is critical for long term normal operation of the equipment. Therefore:

   i. The operational status of the fan shall be checked to ensure that the fan runs in a stable manner, at a regular rotation speed, and buzzes continuously without strange sound

e) **The Dustproof Unit** (if available) shall be cleaned. If not available, then dust shall be removed through suction (not blowing)

f) **The Groundings/Earthing**

   i. The grounding system shall be checked to confirm that it is fastened and satisfies the grounding resistance.

g) **Service Inspection / Bit Error Test**

   i. Periodic sampling test on traffic channels shall be carried out, on condition that no current operating service is affected

   ii. Idle traffic channels between two sites shall be tested to check the channel quality

   iii. In case of no idle traffic channel, the channel originally used for protection shall be temporarily disconnected and used for the test

   iv. In case both of the above are not available, then the EMS software shall be used to query the service performance and alarms, and ensure the quality of traffic channels between the two sites

   v. In all tests above, no bit errors shall be expected.

h) Optical Power Test

i. Using an optical power meter, the transmitter power from the local optical board shall be measured and compared to the original commissioning value. The receive power from the remote optical board shall as well be measured and compared with the original optical budget calculations when commissioning the link.

36.5.4.1.3 SCADA Link Management & Support

SCADA communication links are very vital and therefore their availability shall be 98.5% (maximum of 0.125% per month). Whenever the visibility of any of the substations is lost at the National Control Center (NCC), the following steps shall be followed:

1. The operator at NCC shall immediately inform the Principal Communication Engineer (PCE)
2. The PCE shall immediately appoint technical personnel to troubleshoot the outage and with a view to restore communication and report back.
3. The appointed personnel shall carry out a thorough diagnosis and rectify the problem. This shall involve the following:
    a. Remotely troubleshoot with the station attendant (if available)
    b. If not yet restored, then the whole communication link shall be tested for quality and continuity using a Bit Error Analyser (BEA). If this test is successful, then a report to the PCE shall be compiled
    c. If the above test is unsuccessful, then the link shall be segmentalized and tested using the BEA until the faulty segmented is isolated and corrected
    d. Documentation of the whole process should then be done and a technical report written to the PCE through the SCE.

36.5.4.1.4 Precautions

1. The technical personnel shall be well trained to maintain and trouble shoot the communication links. Refresher courses shall be periodically carried out as well.
2. The technical personnel shall be well facilitated with tools, vehicles and financial resources
3. Thorough and updated documentation of the terminations shall be maintained. As built documents (for new projects) shall also be handed over from the projects department.

4. All technical manuals and wiring drawings shall as well be handed over (for new projects) and new ones generated in case of changes to the existing ones.

37 Guidelines for Technical Specifications & Design Procedures

37.1 Design Principles for Optic Fiber Links

The following general principles shall be considered during the design stage:

i. The network(s) and network equipment types to be used. The options for the equipment are:
   a. PDH, SDH, DWDM, MPLS-TP, etc.
   b. The options for the networks are: a spur, an extension of a spur, a completion of a ring, or a full ring.

ii. The length/distance of the links.

iii. The installation methods of the cable. The options are:
   a. Underground
   b. On wooden poles or tower structures - ADSS, OPGW, or SKYWRAP

iv. Placement of the splice points. Consideration shall be placed on the length of the drums, the markets for either dark fibres or telecom capacity.

v. The testing procedures, including the theoretical expectation, the pre-installation tests and the commissioning tests.

vi. All relevant documentation

vii. All relevant standards.

37.1.1 Loss Budget Calculations

These calculations shall determine the correct transmission power, sensitivity and transmission capacity of the telecom link. Below are the considerations:

a. The power budget – The difference between the transmitter output power and the receiver input power.

b. Loss budget – The sum of the losses of all components used in the cable plant. The cable plant loss shall be within the power budget of the link. It shall also be used to determine the appropriate loss for the cable plant for testing purposes.

37.1.2 Batteries

The recommended specifications are as below:

i. Type - Alkaline batteries, flooded (for well-ventilated areas, e.g. battery rooms in substations), and sealed (for fully enclosed areas, e.g. data centres).

ii. Autonomy – Ten hours (under normal operational consumption). The total peak load of the bus does not normally last more than 10 seconds

37.1.3 Sizing of Batteries

i. Summation of all the loads shall be carried out. The consumption shall be categorized into: Normal Operation Consumption & Total Peak Consumption

ii. The following factors shall be considered during the sizing: Nominal system voltage, Maximum system voltage, Minimum system voltage, Minimum Temp., Nominal Temp., Maximum Temp., Aging factor, Design margin, Charge method & Intensity profile

iii. The standards IEEE 1115 and IEC 62259, as well as the Battery manufacturer's manual shall then be utilized to calculate the optimal capacity of the battery bank.

37.1.4 Battery Chargers

The recommended specifications are as below:

i. Type

a) Thyristor/Thytronic chargers. This is resistant technology that is suitable for industrial environments like substations with high temperatures, prone to dust and high EMI characteristics.

b) Switched Mode Power Supply chargers. These are ideal and optimal for non-industrial environments that are dust free and well air conditioned like offices and data centres

37.1.5 Sizing of Battery Charger

i. The capacity of the charger shall be determined by the summation of the following currents:

a) The total current under normal load consumption

b) The current required to recharge the battery bank (following battery manufacturer's recommendations)

ii. The following standards shall be followed when determining the capacity of the battery charger:

    a) IEC 62259
    b) IEEE 1115

37.2 Standby generators

The recommended specifications are as below:

i. **Type**

   a) Prime vs Standby – This determines whether or not the generator will be the main source of power (prime – no connection to the utility, or where the generator is going to run for more than 250 hours annually) or to be deployed in emergency situations only, for limited duration (standby – no more than 200 hours annually). The load factor for the standby generator is not more than 80%, whereas that of the prime generator is no more than 70%.

   b) Portable vs Stationary – This depends on the application of the generator. At least one portable generator shall be procured or able to be hired as fast as possible when required (failure of the stationary ones at site that will take more than one day of repair)

ii. **Single or Three Phase** – it is standard practice to install three phase generators for industrial purposes or where there is likelihood to have three phase loads. Single phase generators are mostly for domestic purposes

iii. **Brands** – it is recommended to select brands whose support (in case of original spare parts and service) is readily/locally available.

iv. **Single vs paralleling** – The bigger the generator, the better it is to split the burden between two or more smaller generators.

37.2.1 Sizing of Standby Generators

iii. Summation of all the loads that are going to be powered by the generator shall be carried out. The consumption shall be categorized into: starting wattage and normal running wattage. The starting wattage shall be the basis upon which the capacity is calculated.

iv. A load factor of 70% - 80% (for standby gensets) and 60% - 70% (for prime gensets) shall be considered after acquiring the summation of the loads.

v. A design margin of 20% - 30% shall be considered as well to cater for: derating or under performance due to adverse environmental issues such as high temperatures and altitude

vi. Other issues to be considered are:

- Fuel consumption – the bigger the generator, the higher the consumption. Above 250KVA, an external fuel tank (preferably underground) to cover seven days of the generator running, shall be considered
- Conditions and access to site shall as well be thought off.

37.3 Multiplexers (ADMs)

The services that are currently carried on the ADMs (SDH & PDH) listed in order of criticality are:

i. SCADA data between the National Control Center and the various substations

ii. Tele-protection and Differential protection between the various substations

iii. Voice (telephone) and video (surveillance & video conferencing) data throughout the UETCL network (including offices, substations & National Control Center)

iv. Tele-metering data between all metering points (generation and distribution boarders with UETCL) and the protection section premises

v. Corporate LAN network to the various premises of UETCL (Headquarters to Lugogo yard to Control Center to all substations)

For the DWDM network, in order of criticality is:

i. Telecom capacity leased to clients (currently 90Gbps)

ii. Corporate LAN network to the various premises of UETCL (Headquarters to Lugogo yard to Control Center to all substations)

The following should be noted and followed:

i. Service Integrity & Data Loss - The ADMs shall be able to deliver/transmit the information without degradation, loss and on-purpose alteration. This refers to the integrity of the of the services. It is measured by the average of the Bit Error Rate (BER). The links shall be tested for this at the commissioning phase and periodically during operation.

ii. Availability & Dependability – Availability is the percentage of up time of the service.it is the percentage of time that the network can effectively forward traffic. The availability shall be follows:
    a. Protection – 99.0%
    b. SCADA, operational voice – 98.5%
    c. Data service – 98.0%

For low duty cycle operation-critical services (like protection & SCADA communication), it is more appropriate to use service dependability. It is the conditional probability of a service being available when it is solicited. The general availability could be high when the dependability is lower.

Currently the multiplexers/ADMs on the UETCL network are listed below:

DWDM

i. ZXONE 9700

SDH

i. ABB FOX615
ii. SIEMENS HIT7025
iii. TTC MARCONI
iv. UMUX 1500
v. ZTE ZXMP S385

PDH

i. SIEMENS FMX
ii. UMUX 1300
iii. ZTE PCM

The factors below shall be considered during design/provisioning:

i. The process of network planning, communication requirements assessment, and management process design shall be continuous and iterative. There shall be continuous examining of time scales, technological and economical surveys, and organizational and regulatory evolutions.
ii. The substations shall be accessed in a cost effective manner through a dedicated telecommunication infrastructure using optical fibres over HV lines. Considering the peripheral location of many of the HV substations, an external telecom operator is not always in position to provide access with the required capacity.
iii. A small variety in the brands of the ADMs is recommended, however it shan't be big. The diversity in the brands listed above is sufficient. It is recommended that for further network expansion, only the list above shall be considered. The specific one shall depend on which segment of the network is being expanded.
iv. The dependability of a connection is determined by the number of switching and transit nodes it crosses. Therefore, direct inks through dedicated fiber over the HV lines shall be preferred for critical applications.
v. Fault tolerance of the network shall be considered in the design. This is possible by establishing two independent routes between two access points of the network.
vi. The national control center (to which a lot of the communications converge) shall be at the center of the communications network, and not a secondary spur.
vii. The throughput of the communication network, i.e. the allocated bandwidth across the telecom media shall be examined through the sharing scheme of the common communication resources among the concurrent applications
viii. Deterministic and controlled time behaviour for the communications of time-sensitive applications (e.g. SCADA, differential as well as tele-protection) shall as well be considered. Time performance shall be adopted to the requirements of each application through an appropriate choice and blending of technologies and proper topographical structuring
ix. The telecommunication infrastructure shall not compromise the security level that the services infrastructure (SCADA, Relays, LAN) have achieved. The following shall be implemented to ensure security:

a. The physical access point to the ADMs shall be secured possibly allow a network access user authentication (e.g. RADIUS server)
b. The connectivity service across the network shall be isolated from other services through dedicated bandwidth or separate VPNs or VLANs. Security barriers, intrusion detection and encryption shall as well be implemented.
c. The telecom network management platform is a major vulnerability. Access to this platform shall be secured through physical protection, authentication and log management.
d. Secured HMIs, disabling of unused ports, restricting remote configuration and parameter setting are also common measures that shall be implemented.

x. Future proofing, legacy support and vendor independence technologies shall be considered.

xi. Electromagnetic and Environmental constraints shall be considered. This is in light of the fact that the telecommunication equipment is installed in substations. The equipment cabinets shall be closed, fitted with accessories such as: earth bar, surge protection, EMC filters, and wired according to substation installation codes and practices. The impact of Earth Potential Rise (EPR) during station earth fault shall be taken into account.

xii. Service Survivability, resilience and Disaster Readiness. This refers to the ability of the telecom infrastructure to provide and maintain an acceptable level of the service in presence of faults. This shall be provided for in the design. It shall involve the following:
a. Duplication of the core components and access equipment at critical sites
b. Survivable topology, e.g. rings & mesh structures & allowing alternate routing.
c. Disruption tolerance through protection switching and service restoration mechanisms
d. Cost Consideration. The budgetary constraints in the entity shall be considered while designing the telecom/ADM network.

38 Digitization Policy

38.1 The Policy

i. An Electronic Document Management System shall be used as the key digitization and document sharing tool to ensure that UETCL manages its information and records sources in an appropriate, secure, efficient and economic manner.

38.2 Objectives

i. Reduce on time taken to search and access company documents.

ii. Reduce on the risk of misplacing critical documents.

iii. To develop and promote best practice and legal compliance in the creation, use, maintenance and disposal of digital information and records sources.

iv. To develop and promote best practice in the preservation, enhancement and use of modern digital archives and online electronic registry

v. Mitigate the risk of losing vital company information in case of fire, theft, flooding etc.

vi. Provide improved centralized organization-wide receipting and accessibility to documents from anywhere while maintaining high security measures.

vii. Setup a centralized digital registry and work with less and less paper company wide.

viii. To co-ordinate the selection and offering of records and material to UETCL archives, thereby accumulating a digital corporate memory for UETCL that is safe and secure.

38.3 Scope

i. This policy applies to all official UETCL documents of all types and sizes originating from both internal and external stakeholders destined for both internal and external purposes. Historical, current and live documents inclusive.

38.4 Responsibilities

i. The Manager ICT shall be responsible for the security and risk management of the entire digitization process.

ii. PITO shall be responsible for implementing security controls, online workflows and setting up and maintaining the digitization infrastructure and electronic registry and thereafter training and sensitizing end users about the set controls and related trends from time to time.

iii. It is the responsibility of every user of the ICT system to ensure that they utilize the digitization platform to the maximum so as to achieve UETCL corporate objectives.

iv. MHR&A shall be responsible for archiving, management and retrieval of the hard copies upon their digitization and uploading to the electronic document management system.

38.5 Procedures and Control

i. All hard copy official documents initiated from external sources shall be received at the electronic registry office where they will be scanned and directed to predefined workflows for internal processing using the electronic document management system.

ii. The remnant hard copies from the above process in (i) above shall be kept at the registry for not more than one month before being moved to the hard copy archive

iii. ICT system users shall use the electronic document management system as a central repository and online document sharing and collaboration centre for all official documents.

iv. Scanned and/or soft copy documents shall be an acceptable means of communication i.e. submission of a scanned soft copy shall be sufficient for decision making unless so required by the law or any other such statutory requirement.

v. Staff shall not keep hard copies in their custody for more than a month without scanning and uploading to the EDM and submitting the remnant hard copy to the UETCL hard copy archive at Lugogo. This excludes procurement related files whose processing is governed by the PPDA Act.

vi. The UETCL electronic registry will be manned and operated by dedicated registry staff who have been fully trained in the use of relevant equipment and software.

vii. The official format for digitized documents shall be PDF/A diversion from the same shall only be upon approval by MICT

viii. PITO shall enforce reliability, security, licensing compliance and continuity of the electronic document management system in accordance with the prevailing internal ICT Service Level Agreement.

39 Green ICT Policy

39.1 The Policy

i. All technologies implemented on the UETCL ICT platforms and the corresponding usage behaviour shall strive to reduce the environmental impacts associated with information and communication technology (ICT). Green ICT shall be at the forefront of all initiatives and practices.

39.2 Objectives

i. To reduce energy demand in data centres through virtualisation, centralisation, cooling optimisation and the use of renewable energy where practicable.

ii. To assess and classify data centres, offices and equipment rooms in a bid to ascertain their total energy consumption and thereafter implement energy control measures.

iii. To implement green ICT procurement practices in liaison with the equipment and service suppliers.

iv. To establish green ICT resourcing rules for managing new and existing ICT resources.

v. To leverage ICT, such as video conferencing equipment, to enable affiliates to be greener.

vi. Implementing responsible ICT disposal practices, including the re-allocation and re-use, refurbishment and recycling of ICT equipment.

vii. Encouraging green ICT behaviour through training and awareness-raising campaigns.

39.3 Scope

i. This policy applies to all ICT acquisitions, procurements, implementations, maintenance and end user practices in all locations and at all administrative levels.

39.4 Responsibilities

i. MICT shall be responsible for the overall green ICT management and enforcement including facilitation to ensure green ICT is implemented and appropriate resources allocated.
ii. PITO shall be responsible for implementing, maintenance and support of green IT systems and the related infrastructure.
iii. Pr. Com Eng shall be responsible for implementing, maintenance and support of green telecom systems and the related infrastructure.
iv. Pr. Ctl Eng. shall be responsible for implementing, maintenance and support of green power control systems and the related infrastructure.
v. ICT systems users shall be responsible for practicing green ICT in their individual capacities and as far as practically possible.

39.5 Procedures and control

i. All ICT specifications for acquisition of equipment, infrastructure components, software, applications and/or solutions shall incorporate elements of green ICT with a consented effort to control the impact on the environment.
ii. For legacy systems and ICT solutions, suppliers shall be engaged to retrospectively reduce the environmental impact of their supplies to the UETCL environment and throughout the related supply chains.
iii. UETCL will strive to purchase sustainable, efficient products and services and proactively manage and reduce greenhouse gas emissions across the ICT platform.
iv. Sharing and reusing of infrastructure and services across UETCL shall be the best practice through initiatives like cloud computing, online file sharing, digitization and video teleconferencing.
v. Server rooms, data centres, equipment rooms and control centres shall be rationalized through technologies such as virtualization, modern cooling systems and power optimization strategies.

vi. End user devices and peripherals including, amongst others, desktop PCs and laptops, mobile and smart phones, tablets, printers, scanners, copiers and fax machines shall be specified, procured and installed with international green ICT standards considered.

vii. ICT contracts shall put into consideration green "total costs of ownership" including energy, disposal and service delivery approaches.

viii. End users shall turn off equipment at night, print as much less as possible, use email instead of sharing hardcopies, digitize and archive paper work as advised by the digitization policy in this manual.

ix. Most if not all services and transactions shall be processed using the online ICT platform.

40 ICT policy implementation

40.1 Responsibilities of policy implementation

The Manager ICT, in conjunction with the ICT steering committee, shall be responsible for implementation of this policy and procedures manual. All UETCL staff using the ICT Infrastructure, systems and services shall comply with the policies and procedures herein. The PITO, Pr. Com Eng and Pr. Ctrl Eng shall closely monitor the usage and operation of the ICT infrastructure within this policy framework so as to advise the MICT and MHRA regularly on its violation. Implementation of this manual will be through systematic means and interaction with ICT system users who will be required to comply to its provisions.

40.2 ICT Status Reviews

During the course of implementation of this policy and procedure manual, ICT status reviews shall be done at least annually by both internal and external professional information system auditors to assess ICT systems vulnerability, adequacy, suitability and effectiveness of the policies and adherence to NISF standards.

40.3 Staff Sensitization on the policy

The initial orientation notwithstanding, all staff shall be appropriately sensitized on this manual. The new staff will be sensitized on these policies and procedures during their orientation period immediately after reporting for duty. This manual shall also be distributed to all UETCL staff, displayed on UETCL intranet/dashboard and placed on the shared drive on the network for ease of access at all times.

40.4 Policy continuity

This set of ICT policies and procedures are dynamic and may, where necessary, be modified by the ICT steering committee every after three years to meet the institutional emerging ICT requirements.

40.5 Employee's statement of understanding

All users of UETCL shall be required to receive, read and understand this manual. All users shall undertake to comply with the consequences of violating these policies and procedures using ICT Form 10 in Appendix X, which shall be returned to the MHRA duly signed and acknowledged. The employee statement shall be deemed to be a legally binding undertaking to UETCL.

40.6 ICT Policy Review and Update

This ICT policy manual shall be reviewed and updated at least every three years to cater for any changes in the ICT environment.

40.7 Exceptions to policy

In instances where there is a justifiable business need to perform actions that are in conflict with these policies and procedures, UETCL recognises that the policies and procedures created and enforced may not address all the business issues. In order to provide flexibility in these instances, the guidelines in this "Exceptions to Policy" detail the actions that are required to obtain a waiver from compliance to a specific policy.

i. Any exception due to circumstances deemed peculiar and may not require conformance to part or the whole of this policy , approval of a waiver shall be provided by MICT in consultation with the steering committee.

ii. When ICT is a component of a system where the principal function is not ICT, then the provisions of this part shall only apply to the ICT components which have a user interface or transmit information.

iii. In cases of a risk in the use of biometric or any such modes of security enforcement, the identified mode shall be officially waived by MICT in consultation with the steering committee. E.g. With the COVID pandemic the use of finger scanning for door access is discouraged.

Appendix I - ICT Form 1: Equipment Transfer form

UGANDA ELECTRICITY TRANSMISSION COMPANY LTD

ICT EQUIPMENT TRANSFER FORM

Ref____________ **Date______________**

A Equipment Details

No	Items Descriptions	Serial /No.	Asset code	Source Department	Destination

B) Equipment transfer approval
Reasons for transfer of equipment:

……......

……......

.... …………………………………

………..

Initiated by : __________________ Recommended by: ________________ Approved by __________________
(ICT staff) **Head of department** **Manager ICT**

C) Receipt of equipment

Equipment Received by: ……………………….. Names …………………….………..Date of receipt …/……/……

Date to be return:……/……/……

D) Return of equipment

Equipment received back in good and satisfactory condition by (ICT staff):

Sign: ……………..…………….. Name: …..……..……….…... Title: ………….……….. Date: ……/………/……..

Note: The recipient of the equipment shall be responsible for its security and safety and shall bear the full cost incurred by UETCL in the event of loss or damage of the equipment subjected to Section 5.9, sub-section (h) of the UETCL Human Resources manual.

41 Appendix II - ICT Form 2: Equipment Allocation form

UGANDA ELECTRICITY TRANSMISSION COMPANY LTD IT SECTION

IT Equipment Allocation Form

SECTION A: EQUIPMENT DETAILS		
1) Equipment Name:	2)	Serial Number/ Service Tag:
3) Make:	4)	Model:
5) UETCL No.:	6)	Barcode Number (B/N):
7) Date of Purchase:	8)	Supplied by:
9) Contract/Procurement No:	10)	Remark/Comment (Brand new, transferred, leased):
11) Warranty Start Date:	12)	Warranty End Date

SECTION B: EQUIPMENT ACCESSORIES/COMMENTS					
	Bag		Lock		Power Adapter
	Monitor S/N:		Key board S/N:		Detachable Speakers S/N:
	Charger		Headphones		Mouse
	Other Specify:				

SECTION C: DETAILS OF RESPONSIBLE PERSON	
1) NAME:	**2) AC/NO:**
3) DESIGNATION:	**4) LOCATION/WORKSTATION:**
5) SECTION:	**6) REMARK/COMMENT:**

[ ] I received the equipment in good and working condition

[ ] I undertake to use the equipment as per the ICT policies and procedure manual

[ ] Am responsible and hereby undertake to take due care of the above equipment

Signature:______________________ **Date:**________________________

For Official Use Only

Equipment Delivered by:	**Allocation Authorized by:**
Delivery Date:	**Authorization Date:**
Comments:	

42 Appendix III - ICT Form 3: Equipment Movement form

UGANDA ELECTRICITY TRANSMISSION COMPANY LTD

EQUIPMENT MOVEMENT FORM

Date……………………………….

Equipment type……….

Serial No……….

……

…….

……

……

Taken by …….

Name ………

Company……

Section………

Signature……

Reason for movement

……

Movement Authorised by ……………………………………………………………………………………………………….

Name……….

Signature……….…..

43 Appendix IV ICT Form 4: Equipment Inventory

UGANDA ELECTRICITY TRANSMISSION COMPANY LTD

ICT EQUIPMENT INVENTORY FORM

No	Items Descriptions	Model	Serial No.	Manufacturer	Asset Code	Date of Purchase	Supplier	Location	User

Prepared by: ______________________________ **Checked by:** ________________

Name : _________________________________ **Name** :_________________________

Date : _________________________________ **Date** :__________________________

Approved by: ______________________________

Name : _________________________________ **Date** : ____________________________

44 Appendix V -ICT Form 5: Software Inventory

UGANDA ELECTRICITY TRANSMISSION COMPANY LTD

SOFTWARE INVENTORY FORM

No	Software Descriptions	License Code	Date of Purchase	Supplier (Author)	Location	User Dept.

Prepared by: ______________________________

Name : __________________________________

Date : __________________________________

Checked by: ___________________________________

Name :____________________________________

Date :____________________________________

45 Appendix VI- ICT Form 6: Approval of installation and use of new software

UGANDA ELECTRICITY TRANSMISSION COMPANY LTD

APPROVAL OF INSTALLATION AND USE OF NEW SOFTWARE SYSTEM

Ref____________ **Date______________**

A) New Software details:

No.	Software Description	S/No.	Author of Software	User: Name & Sign

B) Software installation and use approval

Reasons for installation of new software:

……

……

……

Recommended by: ________________ Date: ________ Approved by____________ Date: ________

Manager (User Dept.) **Manager ICT**

C) Software installed and tested on _____________________________

(System location)

Software installed and tested by (ICT Staff): **Sign** …………………………………………

Name …………………………………………

Designation: ……………………………………

Date: …………………………………………

Appendix VII - ICT Form 7: Approval to access ICT Systems

UGANDA ELECTRICITY TRANSMISSION COMPANY LTD

APPROVAL TO ACCESS ICT SYSTEMS APPROVAL TO ACCESS ICT SYSTEMS

Ref_____________ Date_______________

A) Details of Person:

No.	Name:	Check No.	Signature	Recommended by: (Name & Signature of Supervisor)

B) Access approval (indicate): IT Room/Network resources/Email/Internet/Other ( )

Reasons for granting access :

………

………

………

………

Recommended by: ______________ Date: _________ Approved by: _____________Date: _________

Manager HRA **Manager ICT**

C) IT system access granted by _________________________________

Name: ……..……..………..…..…………

Designation: ……….............................

Date: …………………….…..…………..

46 Appendix VIII - ICT Form 8: Approval to Connect Own Device to UETCL Network

UGANDA ELECTRICITY TRANSMISSION COMPANY LTD

APPROVAL TO CONNECT OWN DEVICE TO UETCL NETWORK

Ref_____________ **Date_______________**

A) Details of Person:

No.	Name:	Device Name	Signature	Recommended by: (Name & Signature of Supervisor)

B) Approval of own device connectivity to UETCL Network indicate:
IT Room/Network resources/Email/Internet/Other ( )

Reasons for use of own device on UETCL network :

……

……

……

……

Recommended by: ______________ Date: _________ Approved by: _____________Date: _________

Principal IT Officer **Manager ICT**

C) Connectivity done by: __________________________________

Name: …...……...………......…………

Designation: ……….............................

Date: ……………………….…..…………..

47 Appendix IX- ICT Form 9: Fiber Optic service order form

UGANDA ELECTRICITY TRANSMISSION COMPANY LTD

FIBER OPTIC SERVICESORDER FORM

1. Company contact details		
Company name:	City	
Address		
Telephone	Email	
Registered Company No:	VAT:	TIN:
2. Technical contact Details		
Name:	Email	
Telephone:	Mobile	
3. Account contact		
Name	Email	
Tel	Mobile	
4. Required fiber services details		
Segment details	No of cores/STMs required	
Segment 1		
Segment 2		
Segment 3		
Segment 4		
Segment 5		
Other		
Other Total band width required		
5. Required co-location services details	**Location**	
Location 1		
Location 2		
Location 3		
Location 4		
Location 5		
Location 6		
Sign (Customer representative)		
Name	Date	

6. Approval

Checked …...………………… 2. Recommended.......................... 3. Approved: …………………..……

(PCE) **(MICT)** **(MD/CEO / DCEO)**

Name …………………………. Name ……………………….. Name ………………………

Date…………………………… Date ………………………… Date: ……………………..

48 Appendix X- ICT Form 10: Acknowledgement of receipt of ICT policy

UGANDA ELECTRICITY TRANSMISSION COMPANY LTD

ACKNOWLEDGEMENT OF RECEIPT OF ICT POLICY

I …………………………………….. (Name), agree that I will abide by the regulations set forth in the above UETCL ICT policies and guidelines. I also agree to the following:

1. I have received a copy of the Uganda Electricity Transmission Company Limited ICT policy and I have fully read and understood the same.

2. I will adhere to the regulations set forth in the subject ICT policy.

3. I have noted that any violation(s) of this policy will be documented and brought to the attention of Manager Human Resources and Administration for disciplinary action. attention of Manager Human Resources and Administration for disciplinary action.

Employee signature: ________________________________

Employee name: ________________________________

Department: ________________________________

Check Number: ________________________________

Date: ________________________________

49 Appendix XI- ICT Form 11: The requirements collection form

UGANDA ELECTRICITY TRANSMISSION COMPANY LTD

The requirements collection template form

A) High level Requirement Detail

Requirement ID	<Unique id #>		**Requirement Type**		<See List Below>		**Use Case #**		<Unique id #>
Status	***New***	<x>	***Agreed-to***	<x>	***Baselined***	<x>	***Rejected***	<x>	
Parent Requirement #	<Enter the unique id #(s) for each requirement that this requirement supports (This field will be empty for high level requirements e.g., business requirements)>								
Description	<Enter concise description of requirement>								
Rationale	<Provide a brief rationale, and or business value for the requirement.>								
Source	<Name of Requirement. Provider>				**Source Document**		<filename>		
Acceptance/Fit Criteria	<Provide a target that makes it possible to test if requirement was satisfied>								
Dependencies	<List other requirement. Id#s that this requirement is dependent on>								
Priority	***Essential***	<x>	***Conditional***	<x>	***Optional***	<x>			
Change History	<List history of changes to this requirement>								

NB: Detailed User Requirement Document Must be attached

B) Collected requirements approval

Major reasons and value to be added by this requirement:

……………………..…………………………………………………………………………..

....

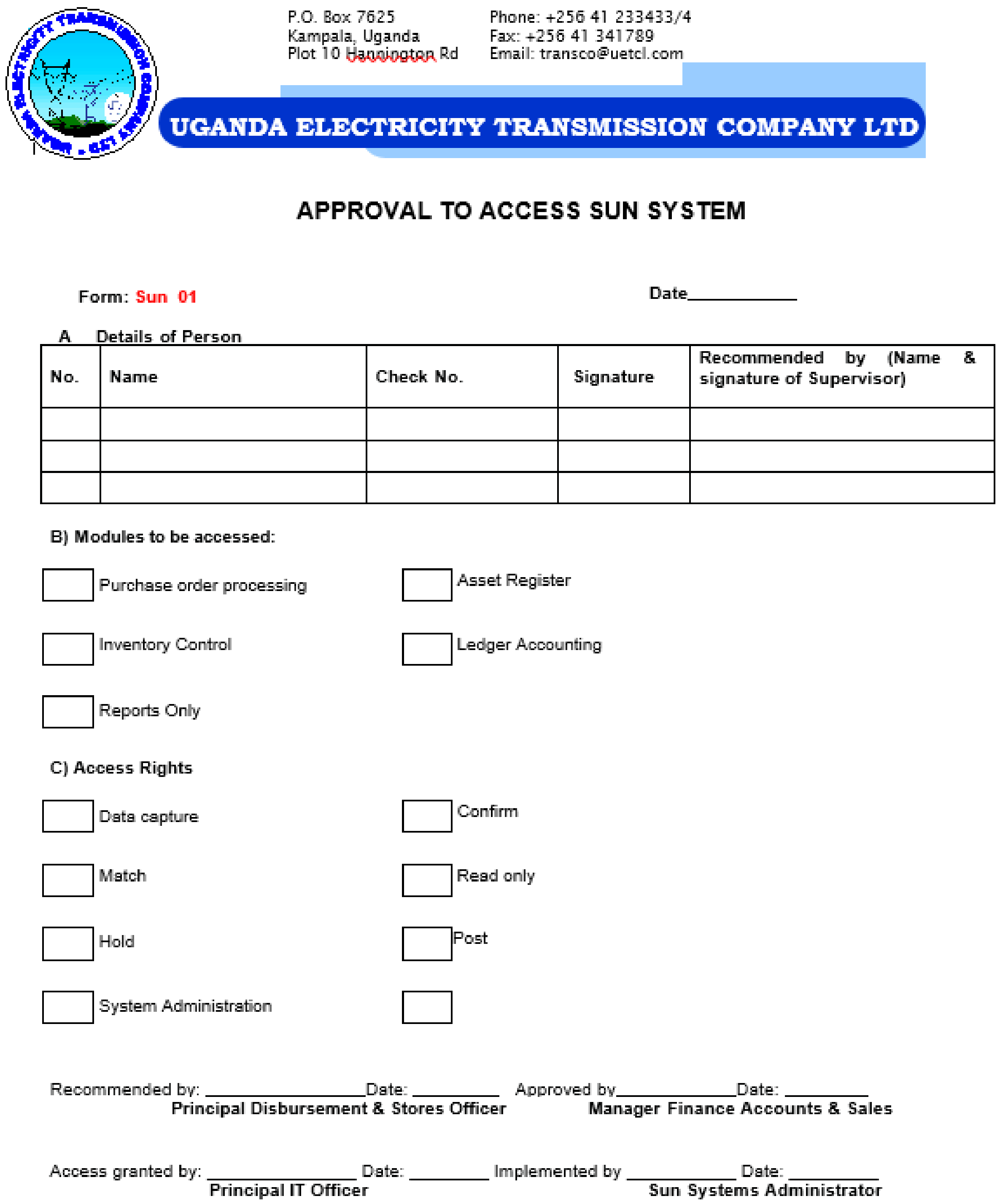
Recommended by: _________________ Date: _________ Approved by_____________ Date: _________
Manager (User Dept.) **(PITO/Pr. Com Eng/Pr. Ctrl Eng.)**

C) Requirement to be tested on ________________________________
(System location)

Requirement solicited/received by (ICT Staff):

Sign ……………..………………..........
Name …..……..…………......…………
Designation: ……….............................
Date: …………………….…………….

50 Appendix XII- ICT Form 12: Approval to Access Sun System



P.O. Box 7625
Kampala, Uganda
Plot 10 Hannington Rd

Phone: +256 41 233433/4
Fax: +256 41 341789
Email: transco@uetcl.com

UGANDA ELECTRICITY TRANSMISSION COMPANY LTD

APPROVAL TO ACCESS SUN SYSTEM

Form: Sun 01

Date____________

A Details of Person

No.	Name	Check No.	Signature	Recommended by (Name & signature of Supervisor)

B) Modules to be accessed:

□ Purchase order processing

□ Inventory Control

□ Reports Only

□ Asset Register

□ Ledger Accounting

C) Access Rights

□ Data capture

□ Match

□ Hold

□ System Administration

□ Confirm

□ Read only

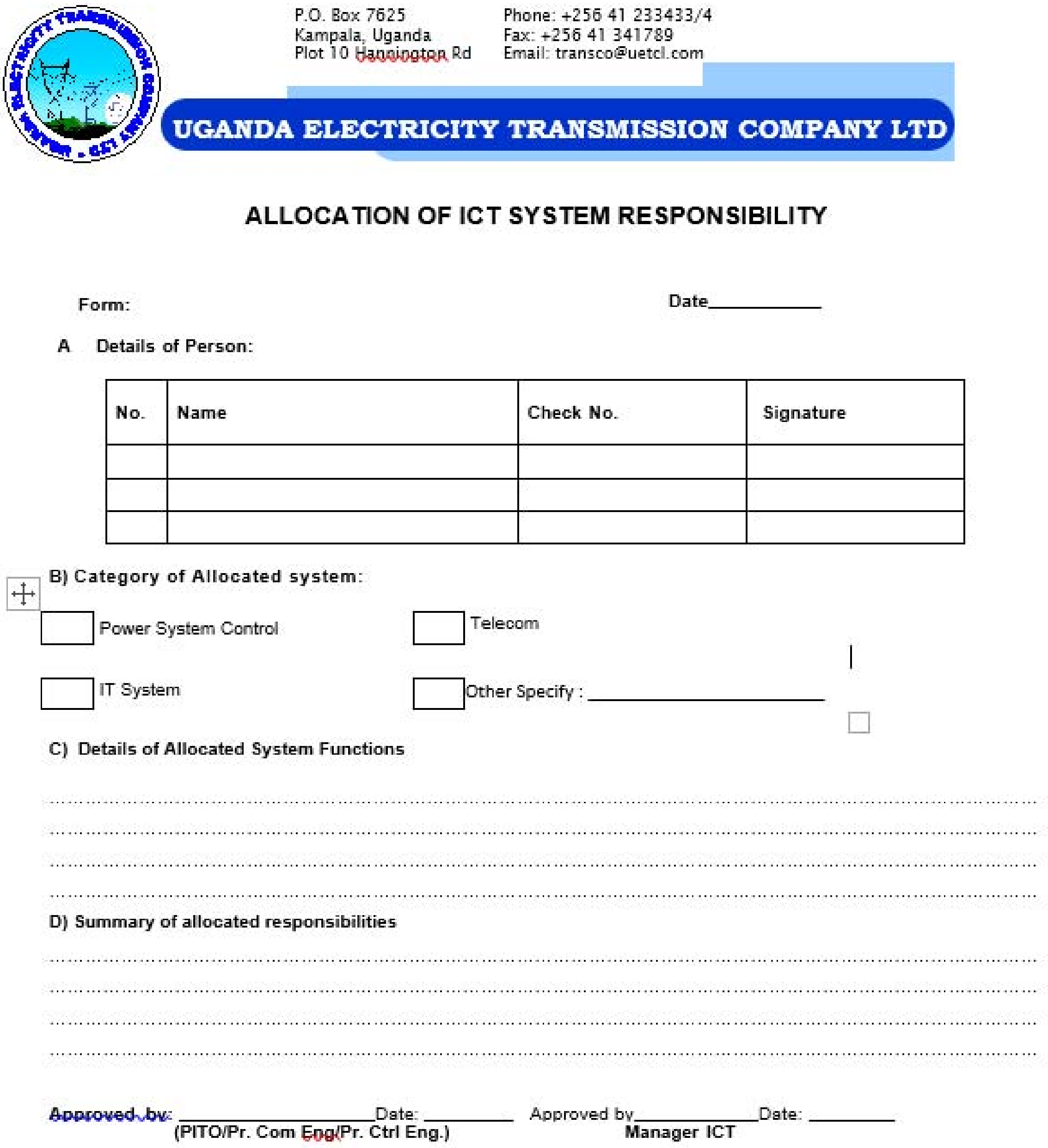
□ Post

□

Recommended by: _________________Date: __________ Approved by____________Date: __________
Principal Disbursement & Stores Officer Manager Finance Accounts & Sales

Access granted by: ________________ Date: ________ Implemented by ___________ Date: __________
Principal IT Officer Sun Systems Administrator

51 Appendix XIII- ICT Form 13: Allocation of ICT System Responsibility



P.O. Box 7625
Kampala, Uganda
Plot 10 Hannington Rd

Phone: +256 41 233433/4
Fax: +256 41 341789
Email: transco@uetcl.com

UGANDA ELECTRICITY TRANSMISSION COMPANY LTD

ALLOCATION OF ICT SYSTEM RESPONSIBILITY

Form: Date____________

A Details of Person:

No.	Name	Check No.	Signature

B) Category of Allocated system:

□ Power System Control   □ Telecom

□ IT System   □ Other Specify : ______________________

C) Details of Allocated System Functions

……

……

……

……

D) Summary of allocated responsibilities

……

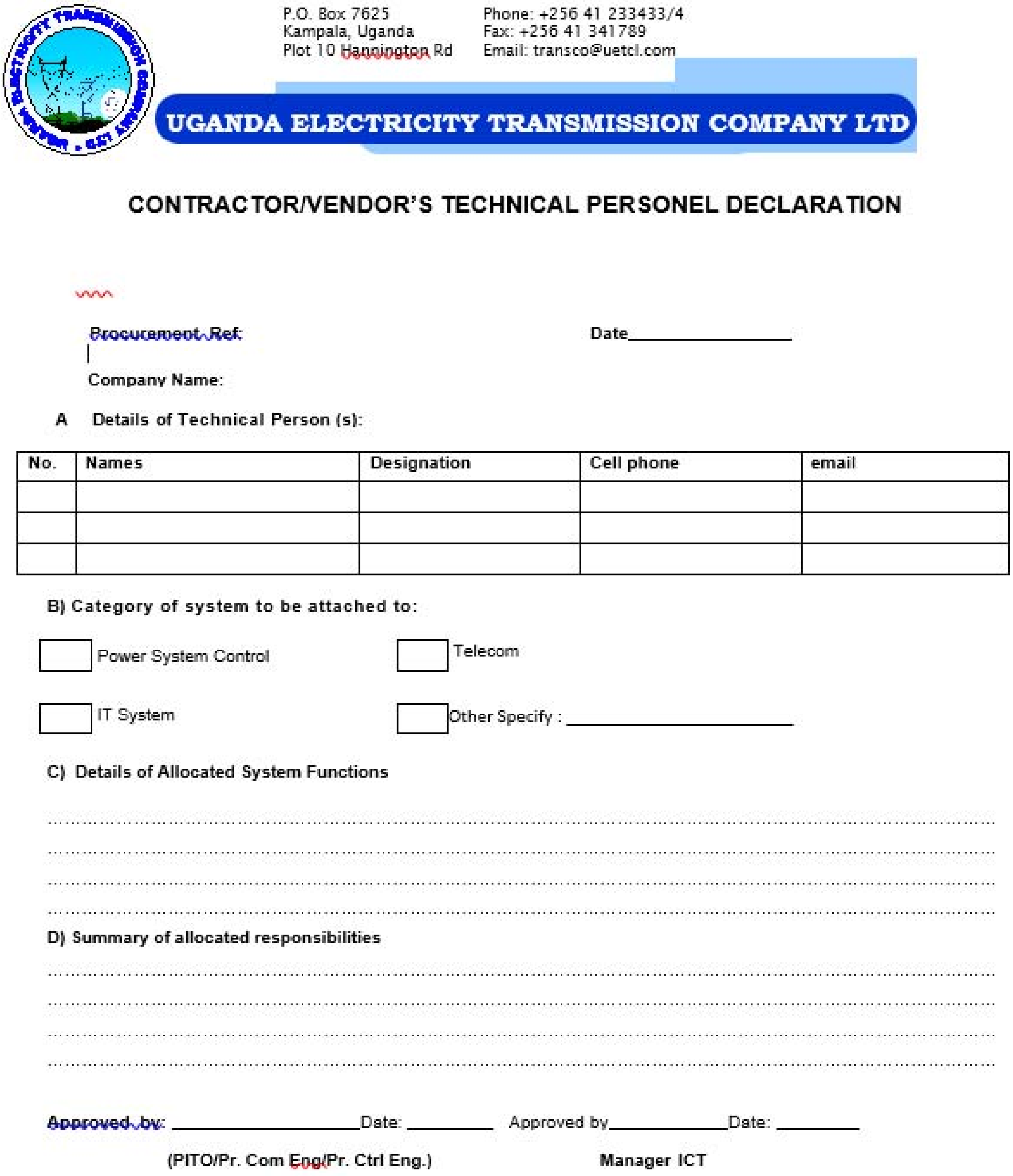
……

……

……

Approved by: ____________________Date: _________ Approved by____________Date: _________
(PITO/Pr. Com Eng/Pr. Ctrl Eng.)   Manager ICT

52 Appendix XIIV- ICT Form 14: Technical Personnel Declaration Form



P.O. Box 7625
Kampala, Uganda
Plot 10 Hannington Rd

Phone: +256 41 233433/4
Fax: +256 41 341789
Email: transco@uetcl.com

UGANDA ELECTRICITY TRANSMISSION COMPANY LTD

CONTRACTOR/VENDOR'S TECHNICAL PERSONEL DECLARATION

Procurement Ref: Date__________________

Company Name:

A Details of Technical Person (s):

No.	Names	Designation	Cell phone	email

B) Category of system to be attached to:

□ Power System Control □ Telecom

□ IT System □ Other Specify : ________________________

C) Details of Allocated System Functions

……
……
……
……

D) Summary of allocated responsibilities

……
……
……
……

Approved by: ____________________Date: _________ Approved by____________Date: _________

(PITO/Pr. Com Eng/Pr. Ctrl Eng.) Manager ICT