Pasiansi Wildlife Training Institute (PWTI)

ICT POLICY AND GUIDELINES

[August 2020]

DOCUMENT CONTROL

Current Document Status			
Version	PWTI-001	**Approving body**	Board of Trustees/Principal
Date	17 August 2020	**Date of formal Approval (if applicable)**	
Responsible Officer	ICT officer if PWTI	**Review date**	
Location	PWTI Head Office		

Version History			
Date	**Version/Document Number**	**Author/Editor**	**Comments**
10 August 2020	PWTI-001	USAID-PROTECT	First Draft of ICT Policy and guidelines for PWTI

Table of Contents

ABBREVIATIONS

BCP	Business Continuity Plan
COBIT	Control Objectives for Information and Related Technology
CD-ROM	Compact Disk Read Only Memory
DRP	Disaster Recovery Plan
ED	Executive Director
E-Mail	Electronic Mail
ERP	Enterprise Resource Planning
HDD	Hard Disk Drive
HOD	Head of Department
HR	Human Resource
ICT	Information and Communication Technology
ICTPG	Information Communication Technology Policy and Guidelines
ID	Identification
IS	Information System
IT	Information Technology
LAN	Local Area Network
PC	Personal Computer
PROTECT	USAID Promoting Tanzania's Environment, Conservation, and Tourism
PWTI	Pasiansi Wildlife Training Institute
UPS	Uninterruptible Power Supply
WAN	Wide Area network

FOREWORD

The adoption and utilization of Information and Communications Technology (ICT) Policy and guidelines within Pasiansi Wildlife Training Institute is aligned to the Institution Strategic Plan. The implementation of ICT Policy and guidelines requires an overall guiding framework to ensure that it's well-managed, complies with legal and regulatory requirements, creates value, and supports the realization of the Institute objectives based on globally accepted best practice, guidelines and principles.

In line with the above, the Pasiansi Wildlife Training Institute ICT Policy and guidelines provides a structure for all the relevant ICT policies to support the achievement of the ICT Vision. Broadly, the policies here within spell out best practice, provide guidance in the delivery, implementation and usage of ICT.

Lastly, I wish to acknowledge the efforts of the PWTI Management and USAID-PROTECT for ICT Support in the coordination of the development of the ICT policy and guidelines for PWTI. We all have an obligation to the Institute to comply with this Policy

……..

Chair

Pasiansi Wildlife Training Institute(PWTI)

1. INTRODUCTION

1.1 Applicability

This ICT policy and guidelines is applicable to all individuals, permanently or temporarily employed within the PWTI**,** including third party contractors, consultants and suppliers with access to PWTI. This will include all Dealers, Franchisees and other parties that offer a service to PWTI or who use PWTI infrastructure. Throughout this policy, all of the above individuals will collectively be referred to as "**Users**". This document does not substitute or in any way affect the validity of the PWTI, Tanzania Code of Ethics.

1.2 Mission of the PWTI

The mission is to produce quality wildlife rangers at operational level to the public institutions and individuals for protecting wildlife resources through offering paramilitary, wildlife management, law enforcement and security training as well as research and consultancy services.

1.3 Vision of the PWTI

The vision is to be the center in providing appropriate training at operational level in wildlife law enforcement for sustainable wildlife Management.

1.4 Purpose

The "Information and Communication Technology Policy and guidelines" set out the principle and standards to be applied to the management of PWTI. Information Technology environments to ensure that all lCT investments are secured, aligned to the overall corporate strategies, plans and acts as a Business Enabler, Support Tool, conduit for innovation within the Institute, and support PWTI to improve its training environment.

1.5 Objective

The overall objective of the *"Information and Communication Technology Policy and guidelines"* is to provide guidance and direction for the Investments in lCT, security, governance, and use of lCT within the Organisation.

The Specific Objectives of this policy are as follows:

a) Protect the investment.
b) Safeguard the information contained within these systems.
c) Reduce Institution and legal risk.
d) Protect the good name of the Institution
e) There are sufficient and appropriate skills to ensure effective lCT
f) To ensure that the Board, Management and Staff are aware of their responsibilities
g) To ensure that lCT investments are aligned with Institution plans

h) The Institution is aware of how lCT can enable its business

1.6 Consequences of Breach

Consequences of Breach for staff will be as per 'Staff and Administrative Regulations', and for external parties as per individual contracts.

1.7 Application

a) The policy will be applied to all IT equipment, infrastructure and software used by PWTI users.
b) Every user of PWTI facilities must read this policy and acknowledge in writing that he/she has understood and will be bound by it.
c) Violations will result in disciplinary action in accordance with PWTI policy. Failure to observe these guidelines will result in disciplinary action by the Institution depending upon the type and severity of the violation, whether it causes any liability or loss to the Institution, and/or the presence of any repeated violation(s).

1.8 Expectations

Through this policy it is expected that the ICT Unit at PWTI will:

a) Operate efficiently through proper staffing and empower staff to deliver expected quality services;
b) Appropriately equip ICT units with necessary tools and facilities.
c) Provide business solutions that will add value to PWTI processes.
d) Provide full support to all IT related processes and users.
e) Meet agreed and specified Key Performance Indicators.
f) Protect its information against unauthorized exposure, disclosure and access
g) Ensure physical safeguarding of valuable information assets
h) Ensure the uninterrupted availability of organizational relevant information
i) Maintain a healthy balance between the cost of implementing ICT measures, controls and the identified risks as well as the possible transfer of such risk.

This ICT Policy and guidelines dated ……replaces all the existing ICT policies.

2. BACKGROUND

The Information Communication and Technology(ICT) in the Institution are provided for the use of PWTI staff in performing their duties. For ICT to bring the desired goals and objectives, policies should be in place to govern business operation. This ICT policy and guideline is about the setting of such governing rules and procedures.

2.1 Contents of ICT Policy and Guidelines

The following are among the key ICT Systems of PWTI:

a) All computers, laptops, servers, tablets, telephones, Local area network(LAN) owned by PWTI;
b) Any network component linking these devices together or the Internet;
c) All peripherals, software, data and media associated with these devices;
d) ICT equipments and other devices forming part of the PWTI data network; Networked reprographic equipment (Printers & Scanners)
e) Software owned or licensed to PWTI

3. IT GOVERNANCE

The PWTI IT Governance is responsible for the administration of this policy.

3.1 Roles and Responsibility

(i) The Principal is accountable to the Board of Directors/trustees for the proper development, implementation and maintenance of this Policy;

(ii) The Board Audit Committee of the Board of Directors is responsible on behalf of the Board of Directors for overseeing development, implementation and maintenance of the ICTPG, and the ICT Officer is responsible for implementing and maintaining the ICT policy and guideline;

(iii) The ICT Officer is responsible and accountable to the Principal for executing the actions required of him by the IT Steering Committee, Principal and PWTI Management;

(iv) Individuals that have specific responsibilities in terms of the ICTPG is identified in the Roles & Responsibilities Register and the Head of HR is responsible for ensuring that the detailed ICT Policy and guideline requirements of individual roles are contained in their job descriptions;

3.2 IT steering committee Roles and Responsibility

The IT steering committee serves as a general review board for major ICT projects and should become involved in routine operations. Primary functions performed by this committee includes: -

(i) Review long and short team plan of ICT Unit to ensure they are in accordance with Institution objectives

(ii) Review and approve the major acquisition of software and hardware within the budget limit approved by board of directors/trustees

(iii) Approve and monitor major projects and the status of ICT plans and budget, establish priorities, approve standards and procedures and monitor overall ICT performance

(iv) Support in development of ICT related policies and standards

(v) Review adequacy of resource and allocation of resources in terms of time, personnel and equipment

(vi) Review and approve sourcing strategies, including insourcing, outsourcing and offshoring of functions

3.3 Compliance

(i) The PWTI Management shall comply with legal and contractual requirements to avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements;

(ii) PWTI employees and third parties shall comply with this Policy and any issued Guidelines thereunder;

(iii) The PWTI shall take disciplinary measures against employees who fail to comply with this policy;

(iv) The PWTI shall take measures against a third party who fail to comply with the ICT security policy in line with formal arrangements established between the PWTI and the specific third party;

(v) The management shall conduct ICT Security reviews to ensure that ICT Policy and guideline are implemented and operated in accordance with the Institution policies and procedures.

4. ICT SECURITY POLICY STATEMENTS

4.1 Organisational Security

a. A holistic approach to ICT security management shall be established, involving the co-operation of and in collaboration with all relevant professionals.

b. Access to the PWTI information processing facilities by third parties should be controlled.

c. Outsourcing Information security management shall be discouraged to ensure confidentiality.

4.2 Personnel Security

a. ICT security awareness shall be provided to all employees in order to enhance awareness and educate them on the range of threats and the appropriate safeguards.
b. ICT security responsibilities shall be addressed at the recruitment stage, included in contracts and monitored throughout the employment duration.
c. Potential recruits shall be adequately screened especially for sensitive jobs e.g. system administrators, database administrators, information security officers.
d. When staff change jobs, their ICT security needs must be reassessed and where necessary a special orientation/training should be provided.
e. All employees and contractors shall be made aware of the procedure of reporting different types of incidents (security breach, threat, malfunctions) that might have an impact on security of ICT assets.

4.3 Physical and Environmental Security

a. All rooms housing ICT equipment must be clean, well ventilated and free from dust.
b. Critical or sensitive information system facilities shall be housed in secured areas, protected by a defined security perimeter, with appropriate security barriers and entry controls.
c. Premises chosen to locate information systems equipment and to store data shall be suitably protected from physical intrusion, theft, fire, flood, and other hazards.
d. Equipment should be protected from power failures and other electrical anomalies. A suitable electrical supply shall be provided that conforms to equipment manufacturer specifications.
e. Power and telecommunication cabling carrying data or supporting information services shall be protected from interception or damage.
f. Utilities installation should be provided and physically separated from data communication cabling in new buildings and other installations resulting from necessity of doing so.

4.4 Securing Hardware, Peripherals and Other Equipment

a. PWTI shall outline entitlement for ICT resources as per user post and function within the Institution.
b. PWTI shall outline proper planning for procurement, distribution, utilization and disposal process of ICT resources. All ICT resources shall be acquired from reliable sources and as per user requirements.
c. PWTI shall outline possible sharing cost modalities for ICT equipment that is permanently issued to users as per entitlement detailed on section a.
d. Employees shall report accidental and deliberate damage to PWTI ICT equipment to the IT Officer as soon as it is noted.

e. Logged on computer equipment should always be safeguarded appropriately especially when left unattended.
f. Physical access to highly sensitive areas such as Data Centre, server rooms and network control rooms shall be controlled with appropriate identification and authentication. Staff with authorization to enter such areas shall be provided with information of the potential risks involved.
g. PWTI shall keep up to date hardware documentation and the same shall be made available to staff who are authorized to support or maintain systems.
h. Employees who are issued with laptop(s) and who intend to travel for business purposes shall be made aware of the information security issues related to laptops and other portable computing facilities and shall be alerted on the appropriate safeguards to be undertaken in order to minimize the risks.
i. All ICT equipment belonging to the PWTI shall carry appropriate insurance cover against theft, damage or loss.

5. COMPUTERS ALLOCATION POLICY

Wherever possible each staff will be provided with, or access to, a networked PC with access to application software as required for the efficient fulfilment of the individual's responsibilities. Generally, peripherals (e.g., laptop, tablets, mobile phone, printers, scanners, etc) will be networked resources shared by multiple users and will not be provided with each individual workstation.

5.1 ICT Inventories

The ICT Unit shall maintain an ICT register of all computer equipment and software, which includes name, specifications, serial numbers/licence, and location of all hardware items or software. Individual Section, Programs and Projects shall be responsible for maintaining the ICT register of all equipment and software under their jurisdiction.

5.2 Computer/Mobile devices Allocation

As a general policy the allocation of mobile devices/computers (desktop and laptop) shall be as follows:

(i) **Servers** - Department, isolated/independent offices, specific functions (e.g. servers hosting specific applications).
(ii) **Desktops -** Standard computer used in offices. All computers will be connected in a network where applicable.
(iii) **Laptops -** Directors, Managers, Head of Department (HOD), Teachers, and other key employees whose duties require them to be moving from one place

to another most of the time and in the process they need to collect and disseminate information.

(iv) **Tablets/Mobile devices-** Directors, Management and student/teacher interact with tablets/mobile devices in the Institution campus/field work which challenges the teacher/student to access learning or teaching materials. The tablets/mobile devices should be flexible interfacing with Institution devices aligned with all security standards of PWTI

6. ICT EQUIPMENT AND SOFTWARE RELATED POLICIES

The following policies relate to adding network lines/network IP addresses, adding additional computers and printers, and computer installations. These policies are necessary in order to control the total costs related to the support and replacement of the computers and related items.

6.1 Additional Equipment

The addition of a computer hardware, software or printer in a program, project or department must be initiated by an appropriate controlling officer or user and approved by management depending on availability of funds.

6.2 Replacing Equipment

The replacement of a computer or software must be initiated by a user, approved by a senior user from the department and the IT Officer should assess the fault, user needs, specification and submit it to Management of General Support Services for approval.

6.3 ICT Change Management

(i) PWTI should document all changes of software and hardware. At a minimum control process the documentation should include:
   a) Registering/initiating change
   b) Analysis by IT team
   c) Authorization of changes
   d) Solution test
   e) Approval for implementation
   f) Review and closure of changes.

(ii) All changes should be documented, authorized and tested in the test environment before implementation to live environment to ensure:
   a) Changes have met user needs
   b) Test results are adequate
   c) Evidence of user approval has occurred

6.4 Equipment Maintenance

(i) All equipment will carry a minimum warranty for defects/support from the supplier. After the warranty period, support will be provided by the IT Unit by using in-house resources or outside contracts depending on the level of maintenance required. Equipment will only be repaired to the tune of 20% of their current replacing value after which value the equipment will be considered for replacement.

(ii) The ICT Unit will carry out routine service and maintenance on all IT equipment twice or three times per six months.

(iii) All computers sent out for repair must have all their sensitive data protected against access. Where possible all folders containing data files must be protected with a password or hard disk drive should be removed.

6.5 Copyrighted Software

Copyright law restrictions prohibiting the unauthorized copying, modification or unlicensed use of software and software documentation, in which copyright is not owned by PWTI must be adhered to.

(i) The Institution shall maintain written records of software installed on each machine and ensure that a license or other proof of ownership is on file for each piece of software;

(ii) Users should not install personally owned software on PWTI equipment unless such software is licensed and its use is approved by the Management.

6.6 Computer and Peripherals Disposition

(i) All programs, projects or department computers, tablets, telephones, printers and related hardware items (equipment) that are no longer needed by a department will be returned to the ICT Unit or Administration office for disposition.

(ii) Equipment that can no longer be used or be economically supported will be classified as **obsolete** and will be disposed of as per PWTI procedures. If disposal includes a working storage media, all data on that media must be destroyed beyond recovery.

6.7 Information Exchange

(i) All documents within the Institution will be prepared using Institution-standard office tools to allow for easy information exchange. The selection of such tools will be determined by the IT steering committee.

(ii) All internal communications (memos, policies, announcements, phone lists, etc) where possible should be passed and stored electronically and not on paper.

7. ICT INVESTMENTS AND ACQUISITIONS

Management shall ensure that all ICT investments are aligned with Institution business strategy. ICT is the organisation enabler, the following standards should be adopted

(i) Management shall develop an lCT strategy that underpins the Institution business strategy
(ii) All lCT investments shall have a business justification and technical support
(iii) The Institution shall adopt a Return on investment approach both in terms of financials and or value added proposition to lCT investments

8. CYBER SECURITY POLICY

Cyber security in this context refers to the protection of PWTI digital infrastructure and information assets against any compromise or attack that may affect its confidentiality, integrity and availability.

8.1 General Use and Ownership Policy

The ICT Unit at PWTI shall

(i) Undertake ownership of all cyber security risks
(ii) Provide leadership for the Governance of Cyber security within the University
(iii) Articulate the University's information risk appetite
(iv) Ensure that the appropriate security controls and mechanisms have been put in place based on a formal periodic risk assessment;
(v) Maintain an updated ICT risk register in line with the following from the National Information Security Framework
(vi) Maintain an updated and tested Business Continuity and Disaster Recovery Plan for all critical PWTI digital infrastructure and information assets
(vii) Implement periodic systems and infrastructure audits.
(viii) Maintain updated and documented secure configurations baselines for all hardware and software
(ix) Develop and implement a patch management plan
(x) Implement network filtering to protect the network against malware related threats
(xi) Ensure the controlled and audited usage of ICT administrative privileges
(xii) Implement monitoring and real time analysis of all ICT network device event security logs with a centralized mechanism
(xiii) Ensure the limited and controlled use of network ports and controls
(xiv) Ensure the implementation of appropriate Wireless Access(WAP) Provision protection mechanisms
(xv) Coordinate and lead the rollout of periodic cross-cutting security awareness and training

(xvi) Ensure all ICT equipment is installed with the appropriate active malware protection that is continuously updated

(xvii) Develop and maintain a handover mechanism for ICT equipment and information during end of staff employment contracts aligned to the PWTI Human Resource Policy

(xviii) All PWTI users shall report any cyber security incident to the ICT Unit

8.2 Network Security

(i) Antivirus software shall be installed on all servers, PCs, Laptops and Tablets/Mobile devices to ensure all data and software received is scanned prior to use.

(ii) Personal computers (e.g. desktops, laptops and notebooks) should be scanned daily for viruses, as part of the re-boot process. Bypass of the inbuilt scanning process is strictly prohibited.

(iii) All information or files electronically down-loaded from the Internet onto a workstation must be scanned before being used.

(iv) All e-mail and their attachments must be scanned before entering the PWTI e-mail system.

(v) If a virus attack is suspected the following must be observed:

a) Suspected removable media must be isolated
b) Suspected PC must not be used;
c) The IT Officer must be informed.

(vi) No disks containing unauthorized data and programs, from outside the organisation can be used on the organisation PC's (i.e., games disks, codes written on home PC's.

(vii) The infected Workstation should be isolated (i.e. physically disconnected from all networks) to prevent future usage until the virus has been removed.

(viii) The IT Officer should be responsible for the removal of the virus and investigation of its origin.

(ix) IT Officer/System Administrators (Hardware and Software) should run antivirus software on all their network file servers on a regular basis (preferably daily).

(x) Any electronic information transferred into the PWTI IT environment via removable media must be scanned before use.

8.3 Bring Your Own Device (BYOD)

PWTI shall allow the usage of personal devices on the Institution network as long as such complies with the PWTI policies and offers a similar level of protection as specified by the Unit responsible for ICT. Such usage will be subject to the following:

(i) PWTI shall have the right to investigate/ audit such devices in case of any malicious activity, cybercrime or fraud that affects the Institution.

(ii) No sensitive or confidential PWTI information shall be stored on such devices

(iii) PWTI will provide an acceptable level of protection for such personal devices as defined by the Unit responsible for ICT from time to time;
(iv) Registered with ICT Unit.

8.4 Access Control

The PWTI shall:

(i) Maintain a smart access control to govern access to all Institution buildings by both staff, students, visitors and contractors
(ii) Define and periodically review the technology for SMART Access control for different categories to take advantage of new ICT innovations
(iii) Implement CCTV for access monitoring of all Institution buildings and entry points

8.5 User ID and Password Policy

This policy will be applicable to only users who are using critical systems of the Institution such as payment system, website and email administrators, examination database, Internal and external portals, government systems and all super user accounts operated at PWTI.

(i) Each user will be given a unique user id to access the Institution information systems that comprises the users first name and full surname. Where two users have the same first name and same surname, these users will be given user ids consisting of their first two initials (first and middle name) followed by their surname.
(ii) Each user will be required to choose a password to access the organisation information systems. This password is to be known only to the individual concerned.
(iii) End user Passwords are not to be written down or disclosed to anyone under any circumstances.
(iv) System Administrators should use administrator accounts purely for administrative issues and should not disclose any confidential information that they may come across in the course of their duties.
(v) If the user authentication technique is based upon passwords:
    a) End users shall be required to change their password after 90 days. Highly privileged (e.g. Users who authorize payments) or System users shall be forced to change their password after 30 days; and
    b) Users must not be allowed to reuse the password within a time frame of 6 months when a change is enforced.
(vi) All passwords for all system users must meet the following complexity requirements;
    a) Minimum of eight (8) characters in length
    b) Mixed characters (numbers, letters and Non-alphabetic characters for example, $, #, %)

c) Mixed Upper case letters (A through Z) and lowercase letters (a through z)
d) Passwords should not be obvious (not contain the user's account name or parts of the user's full name that exceed two consecutive characters) and must be kept confidential.

(vii) All users must terminate their active sessions when finished.
(viii) User accounts must be locked automatically after three unsuccessful login attempts.
(ix) All PCs and Laptops should be set to timeout in 10 minutes when left inactive and lock the screen, the user must be prompted to enter password on resume

9. ACCEPTABLE USE OF EMAIL

Electronic mail (E-mail) is a significant organisation, information and communication tool for the PWTI and employees need to be aware of their personal responsibilities with regards to its use and the potential consequences resulting from misuse. All employees who use the PWTI e-mail system are required to comply with this policy statement.

9.1 Organisation Use

The e-mail system is to be used solely for organisation purposes of PWTI and not for personal purposes of the employees. All PWTI work emails should be sent out and received using PWTI email addresses.

9.2 Ownership

All information and messages that are created, sent, received or stored on the PWTI e-mail system is the sole property of PWTI. Employees are not allowed to copy information and messages to his own private email.

9.3 Prohibited

Below is a list of unacceptable use of Email and Internet service that will be violation to the PWTI ICT Policy and Guideline

a) E-mails may not contain statements or content that are libellous, offensive, harassing, illegal, derogatory, or discriminatory. Foul, inappropriate or offensive messages such as racial, sexual, or religious slurs or jokes, fraudulent are prohibited. Sexually explicit messages or images, cartoons or jokes are prohibited.
b) Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the messages to others.
c) Broadcasting e-mails, i.e., sending the same message to more than 10 recipients or broadcasting e-mails that have no organizational value
d) Knowingly sending or forwarding a mail or an attachment that contains a virus

e) Forge or attempt to forge e-mail messages
f) Send messages using another person's mail account without his/her authorization
g) Copy messages or attachment belonging to another user without permission of the originator
h) Disguise or attempt to disguise your identity when sending an E-mail
i) Set up or operate a Web service connected to the PWTI network without consultation and approval from the IT Officer
j) Accessing web sites that are of no benefit to the Institution, especially when done during work hours
k) Conducting a personal business using Institution resources.
l) Downloading executable files without approval
m) Practice an activity designed to deny the availability of PWTI service or communications resources to others

9.4 Security

The PWTI e-mail system is only to be used by authorized persons, and an employee must have been issued an e-mail password in order to use the system. Employees shall not disclose their codes or passwords to others and may not use someone else's code or password without express written authorization from PWTI. Employees who left the organisation are not allowed to access e-mail systems.

9.5 No Presumption of Privacy

E-mail communications should not be assumed to be private and security cannot be guaranteed. Highly confidential or sensitive information should not be sent through e-mail.

9.6 Certain Prohibited Activities

Employees may not, without PWTI express written authorization transmit trade secrets or other confidential, private or proprietary information or materials through e-mail.

9.7 Message Retention and Creation

Employees should be careful in creating e-mail. Even when a message has been deleted, it may still exist in the printed version, be recreated from a back-up system, or may have been forwarded to someone else. Please note that appropriate electronic messages may need to be saved. And, the Institution may be required to produce e-mail in litigation.

9.8 Viruses

Any files downloaded from e-mail received from non-website sources must be scanned with the virus detection software(anti-virus). Any viruses, tampering or system problems should be immediately reported to (ICT Officer)

9.9 Consequences of Violations

Violations of this Acceptance use of Email policy or other PWTI policies may result in discipline, suspension and even termination of employment.

10. SOCIAL MEDIA POLICY

Social media is referred to as any web software that provides electronic social interaction amongst its subscribers and communities.

a) PWTI Official Social Media Sites:
   (i) Only the PWTI official social media sites will be allowed to make use of PWTI trademarks and symbols
   (ii) Only authorized personnel by the PWTI shall be allowed to make postings on the official social media sites
   (iii) Any information shared across the social media sites shall comply to fair use and comply to PWTI policies in the domains of Conflict of interest and PWTI trademark and symbol protection
   (iv) All information shared across the PWTI social media sites should not make reference to any biased statements on matters such as politics, religion, race, gender, sexual orientation, inter alia; statements that contain obscenities or vulgarities
b) This policy does not apply to the use of social media for educational purposes as referenced in the PWTI E-learning

11. DATA CLASSIFICATION

a) Information shall be classified in one of the following categories, Highly Confidential, confidential, Proprietary, Internal Use and Public document.
b) PWTI shall differentiate information assets which have little value and those one that have high sensitivity and confidentiality. Information can be classified as follows: -
   - Highly Confidential
   - Confidential
   - Proprietary
   - Internal Use Only
   - Public Documents

12. SOFTWARE DEVELOPMENT AND ACQUISITION POLICY

The following statements govern the implementation of this policy

a) The Unit responsible for Software development and acquisition, shall periodically define the Systems Life Cycle methodology for:
   (i) systems and software engineering for both in-house and outsourced development
   (ii) acquisition of off the shelf software
   (iii) maintenance of software
b) All software shall undergo testing and quality assurance before installation in any production environment within the PWTI and ensure provision for:
   (i) Information classification
   (ii) Usage of the least privilege principal
   (iii) Segregation of roles
   (iv) Audit trails
c) All software under this policy shall comply to the Software Licensing and Ownership and Cyber Security Policies
d) All acquired software shall where necessary contain provision for technical support and upgrades
e) All Institution, Departments and units shall where necessary make use of open source software based on a risk based assessment as referenced in the cyber security policy
f) All Institution, Departments, Units undertaking the development or acquisition of any software shall ensure compliance to this policy and plan for end user training
g) This policy does not apply to software development within PWTI for academic or educational purposes

13. CLOUD COMPUTING

(i) PWTI will satisfy that security, privacy, and other ICT management requirements will be adequately addressed by the cloud computing vendor through a signed contract.
(ii) All data or systems accessed over the cloud must be through a secure channel / link for administrative purposes.
(iii) The PWTI shall maintain a copy of all data available in the cloud.

14. BUSINESS CONTINUITY MANAGEMENT

This section outlines measures that have to be taken to reduce the disruption that could be caused by disasters and security failures of ICT systems. The objective is to restore the system at a minimum time possible after such failure/disaster.

In order to ensure business continuity, back up of all critical systems should be maintained. The goal of backups is to prevent the loss of data in case of system failure, accidental deletion of data or accidents such as fire. The following data shall be backed up:

i. Website
ii. All Database operates at PWTI
iii. Accounting System and data
iv. Official Email accounts
v. Servers and All systems operates at PWTI
vi. Network configurations (switch, router and firewall)
vii. Government and Non-Government portal
viii. Electronic teaching materials and Books
ix. Official data and report created by employee

14.1 User data and Database

All PWTI critical databases shall be backed up daily (i.e. every end of business day). A full backup of each system database must be done once a week. For each backup run, each file system should receive a differential backup if it is not having a full backup done.

14.2 System and Server Backup

Full Systems and server backup shall be done at least once in a week or when there is a system change. Backup logs must be maintained to verify such backups.

14.3 Backup Verification

Test restores from backup storage must be performed at least once every month. This ensures that both storage and the backup procedures work properly. Backup verification logs must be maintained.

14.4 Storage Period

Available backup storage must cover a minimum of six months. Ideally backups of systems and server data would go back for about one year and backups of user data would go back about six months. User data should not be archived for long periods of time as it is only being backed up to recover from hardware failure and accidental deletion.

Backups of user data may be stored for a maximum of three years and are to be destroyed or overwritten after that time. Certain information, such as system logs and selected usage logs, should be stored for at least a one year so as to provide data for usage analysis and to help investigate security incidents.

14.5 Storage Access and Security

All backup media must be stored in a secured area that is accessible only to authorized PWTI staff. The media should be stored in a special software fireproof safe when they are not in use. Offline backup hard disk shall be stored at a separate from PWTI Head office (to be determined) in a fireproof safe.

14.6 Off-site Storage

(i) Sufficient backup hard disk (typically be a one-month cycle of backups) to provide a full copy of all information for each critical system must be stored at a location not where the main systems are housed. Off-site storage must be secure and available only to authorized PWTI staff.

(ii) Generally, a rotation schedule should keep a set of Hard Disks on-site until a complete set of data is recorded. Then the most recently completed set of Hard Disk is sent off- site and the set of off-site backups from one month previous is returned. This means that two complete backup sets are stored off- site, so that in the event of a disaster a bad Hard Disk in a backup set will not cause more than a week's data to be lost. For example, the primary site can be in the Mwanza Head office and secondary site can be in different building locations in Mwanza or other region of Tanzania.

14.7 Data Restoration

Data restoration must be supervised by the ICT Unit.

14.8 Data Disposal

All data to be disposed must be erased from data hard disk or any storage media. Hard disk or storage media must be verified that are erased and cannot be read before disposing them. Logs must be kept to verify this disposal.

15. ACKNOWLEDGEMENT OF ACCEPTABLE USE POLICY

This form is used to acknowledge receipt of, and compliance with, ICT Policy and Guideline of PWTI.

Procedure

Complete the following steps:

(i) Read the ICT Policy and guidelines
(ii) Sign and date in the space provided below
(iii) Return this page only to HR

Signature

By signing below, I agree to the following terms:

(i) I have received and read a copy of the: “PWTI ICT Policy and Guidelines” and understand the same;
(ii) I understand and agree that any computers, software, tablets/mobile devices and storage media provided to me by the Institution contains proprietary and confidential information about PWTI and its students, customers or its vendor, and that this is and remains the property of the Institution at all times;
(iii) I agree that I shall not copy, duplicate (except for backup purposes as part of my job here at PWTI), otherwise disclose, or allow anyone else to copy or duplicate any of this information or software;
(iv) I agree that, if I leave PWTI for any reason, I shall immediately return to the Institution the original and copies of any and all software, computer materials, or computer equipment, electronic data that I may have received from the organization that is either in my possession or otherwise directly or indirectly under my control.

Employee signature: _____

Employee name: _____

Date: _____

Department/Section/ Program/Project _____

HR Signature: _____

Name of HR _____ Date: _____