



# **CHINHOYI UNIVERSITY OF TECHNOLOGY**

## **ICT DEPARTMENT**

### **INFORMATION AND COMMUNICATION TECHNOLOGY POLICIES**

March, 2023

Version 2


---

*Amendment number 1 of 2022*

## I. PREAMBLE

---

Information and Communication Technology (ICT) resources constitute a valuable university asset that must be managed accordingly to ensure their integrity, security, and availability for teaching, research, learning, outreach, innovation and industrialization activities. Carrying out this mission requires the university to establish basic ICT infrastructure and to provide both access and reasonable security at an acceptable cost. The university ICT policies and standards are intended to facilitate and support authorized access to university resources and information.

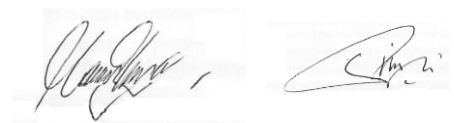


## II. PURPOSE OF THE ICT POLICIES DOCUMENT

---

The purpose of the university Information Communication Technology (ICT) Policies is;

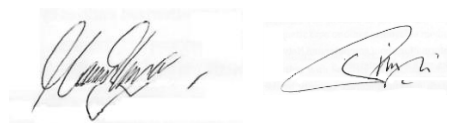
1. To establish university-wide protocol for Information Communication Technologies.
2. To protect the reputation of the university and to allow the university to satisfy its legal and ethical responsibilities with regard to its ICT resources.
3. To protect the user through the provision of procedures for proper use of the ICT facilities.
4. To enable the University to respond to complaints and queries about real or perceived non-compliance with the university ICT policies and procedures.



### III. RESPONSIBILITY

---


Authorized users of Chinhoyi University of Technology Information and Communication Technology (ICT) resources are personally responsible for complying with all university policies, and standards relating to ICTs, regardless of the campus, school, department, centre, location, or access means and will be held personally accountable for any misuse of these resources.



## IV. SCOPE OF THE POLICIES


---

1. These policies apply to all persons that use Chinhoyi University of Technology university-owned, third party-owned, or personally-owned computing resources.
2. These policies apply to all Chinhoyi University of Technology systems and software (both in-house, of-the-shelf developed), user-developed data sets, systems that may access these data, regardless of the environment where the data reside (including systems, servers, personal computers, laptops, portable devices, etc.).
3. These policies apply regardless of the media on which data resides (including electronic, microfiche, printouts, CDs, etc.) or the form they may take (text, graphics, audio, video, voice, etc.).



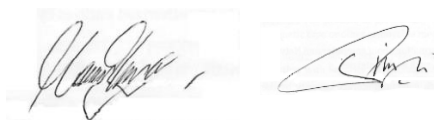
## V. REFERENCE STANDARDS

	Detail	Reference Standard
1	Capacity Management, Demand Management, Network/Service Resilience, Third Party Management	COBIT 5, ITIL, ISO/IEC 20000, ISO/IEC/IEEE 8802-3:2017
2	Service Management	COBIT 5, ITIL, ISO/IEC 20000
3	ICT Governance, Capacity Management, Cloud	COBIT 5, ISO/IEC 17788, ISO/IEC 17789, NIST 500-292, ISO/IEC 19068-1
4	IS and Cybersecurity, Risk Management	COBIT 5, ISO/IEC27000 series, ISO/IEC 38500, ISO/IEC 31000, SP 800-37 Rev. 2
5	Data Centre, Cabling, Network Infrastructure, IT Asset Management, Procurement, Wireless	COBIT 5, TIA-942, ISO 30134, ISO 45001, ISO 41000, ISO 50000, ISO/IEC 19770-5:2015, ISO/IEC/IEEE 8802-3:2017
6	Network Management, Business Continuity, Systems Development and deployment	COBIT 5, ISO/IEC 38500, ANSI/TIA-568, ISO/IEC 11801, ISO 22301
7	Service Monitoring, Service Management	COBIT 5, ITIL, ISO/IEC 20000



# CONTENTS

i.	PREAMBLE.....	i
ii.	PURPOSE OF THE ICT POLICIES DOCUMENT .....	ii
iii.	RESPONSIBILITY .....	iii
iv.	SCOPE OF THE POLICIES .....	iv
v.	REFERENCE STANDARDS .....	v
1.	ICT GOVERNANCE POLICY.....	1
1.1	Introduction.....	1
1.2	Policy Objective.....	1
1.3	Roles and Responsibilities .....	1
1.4	Enterprise Architecture Principle.....	2
1.5	Third Party Management.....	3
1.6	Project Management.....	4
1.7	Audit and Compliance.....	5
2.	ICT SERVICE MANAGEMENT POLICY .....	6
2.1	Introduction.....	6
2.2	Policy Objective .....	6
2.3	Roles and Responsibilities .....	6
2.4	ICT Maintenance .....	7
2.5	ICT Skills and Capacity Building .....	7
2.6	ICT Capacity Building Assessment.....	8
2.7	ICT Capacity building delivery methods.....	8
3.	GENERAL ICT INFRASTRUCTURE USE POLICY .....	9
3.1	Introduction.....	9
3.2	Policy Objective .....	9
3.3	Access to ICT Facilities .....	9
3.4	Acceptable Use.....	10
3.5	Unacceptable Use.....	10
3.6	Termination and or Suspension of User Access .....	12
3.7	Bring Your Own Device (BYOD).....	12
3.8	Control over user activities.....	13
4.	DATA PROTECTION & CLASSIFICATION POLICY .....	14
4.1	Introduction.....	14
4.2	Policy Objective .....	14
4.3	Data Classification .....	14
4.4	Data Classification Diagram.....	15
5.	CLOUD COMPUTING POLICY .....	17
5.1	Introduction.....	17
5.2	Policy Objective .....	17
5.3	Cloud Computing Definition .....	17
5.4	Cloud Management Framework .....	17
5.5	Cloud Risk Management .....	17
5.6	Compliance Assurance.....	17
5.7	Cloud Registration and Management.....	18
5.8	Cloud Usage.....	18
5.9	Recognition of Cloud Service Limitations .....	18



6.	DATA COMMUNICATIONS NETWORK POLICY .....	19
6.1	Introduction.....	19
6.2	Policy Objectives.....	19
6.3	Communication Network Infrastructure .....	19
6.4	Digital Network .....	20
6.5	University Wide Area Network.....	20
6.6	Wireless Access Provision.....	20
6.7	Remote Access .....	21
6.8	Access to Network Infrastructure and ICT Services .....	21
7.	SOFTWARE DEVELOPMENT POLICY .....	23
7.1	Introduction.....	23
7.2	Policy Objective .....	23
7.3	Software Development System Life Cycle.....	23
7.4	Secure Software Development .....	23
8.	CHANGE MANAGEMENT POLICY .....	25
8.1	Introduction.....	25
8.2	Policy Objectives;.....	25
8.3	Change Management Procedure.....	25
8.4	Approval & Deferral of Change.....	25
8.5	Closing a Change Request.....	27
9.	CYBER SECURITY POLICY .....	28
9.1	Introduction.....	28
9.2	Policy Objectives .....	28
9.3	Roles and Responsibilities .....	28
9.4	Proper Use of ICT Resources.....	29
9.5	Password Rules .....	29
9.6	Password Construction Guidelines.....	30
9.7	Physical Security of ICT infrastructure .....	31
9.8	ICT equipment and resources allocated to departments.....	31
9.9	Data Centre/ Server Room Security .....	31
9.10	Access Control .....	31
9.11	Standard Security Configurations for ICT Infrastructure.....	31
9.12	Cyber Security Risk Assessment.....	32
9.13	Vulnerability Assessment and Penetration Testing (VAPT).....	32
9.14	Data Integrity Testing.....	33
9.15	Cyber Security Incident Management.....	33
10.	BUSINESS CONTINUITY AND DISASTER RECOVERY POLICY.....	34
10.1	Introduction .....	34
10.2	Policy Objectives.....	34
10.3	Business Risk Assessment and Business Impact Analysis .....	34
10.4	Prioritization of recovery.....	35
10.5	Disaster Recovery Plans .....	36
10.6	Data Backup Plans.....	36
10.7	Systems log review .....	38
10.8	Contacts and Resources .....	38
11.	ICT ASSET MANAGEMENT POLICY .....	39



11.1	Introduction .....	39
11.2	Policy Objectives.....	39
11.3	ICT Asset Procurement and Registration.....	39
11.4	ICT Asset Classification and Allocation.....	40
11.5	Allocation Classification .....	41
11.6	Replacement of ICT Asset .....	41
11.7	ICT Asset Monitoring .....	42
11.8	ICT Asset Disposal.....	43
12.	ELECTRONIC COMMUNICATIONS POLICY .....	44
12.1	Introduction .....	44
12.2	Policy Objectives.....	44
12.3	Internet and E-mail.....	44
12.4	Creation and deactivation of accounts.....	44
12.5	Prohibited Use .....	45
12.6	Mass Emailing.....	45
12.7	Signatures.....	45
12.8	Monitoring .....	45
13.	SOCIAL MEDIA POLICY .....	46
13.1	Introduction .....	46
13.2	Policy Objectives.....	46
13.3	Social Media Definition .....	46
13.4	Best Practices.....	46
14.	E-LEARNING POLICY .....	48
14.1	Introduction .....	48
14.2	Policy Objectives.....	48
14.3	Virtual Learning Infrastructure .....	48
14.4	Intellectual Property Rights .....	48
14.5	Confidentiality and Privacy .....	49
15.	STATEMENT OF ENFORCEMENT .....	50
16.	APPENDIX A: DEFINITION OF TERMS USED IN THE DOCUMENT .	51

---

# **1. ICT GOVERNANCE POLICY**

---

## **1.1 Introduction**

- 1.1.1 Effective Information and Communication Technology (ICT) Governance provides a conducive environment for the alignment of all ICT investments in a rationalised manner that is aligned towards enabling Chinhoyi University of Technology to meet its goals and objectives.
- 1.1.2 This also contributes to the attainment of value for money, management of risks and effective ICT utilisation.

## **1.2 Policy Objective**

- 1.2.1 To provide centralised and effective Governance of all ICT related matters within the university in a rationalised and harmonised manner.

## **1.3 Roles and Responsibilities**

- 1.3.1 The ICT Department is the focal point of contact for the ICT Service Management function within the university, and shall;
- i. Provide effective ICT support that is responsive to the academic, research and administrative functions of the university
  - ii. Promote effective and appropriate utilisation of ICT resources
  - iii. Contribute towards the sustainability of the unit in order to enable effective execution of ICT Department mandate
  - iv. Promote an environmentally friendly approach to the acquisition, use and disposal of ICT resources
  - v. Coordinate and lead resource mobilisation for counterpart funding for the implementation of the ICT Strategy.
  - vi. Specify, verify and vet ICT standards and procedures aligning them to best practices.
  - vii. Have the overall ownership of the professional and technical mandate of all ICT design and developments, management and maintenance.
  - viii. Operationalize and guide the ICT policy implementation.
- 1.3.2 The university shall establish the ICT Committee that will be a representation of responsible Principal/Head of Department from all the teaching, learning, administration, research domain units and students leadership as a platform for end user satisfaction. With ICT Department as the secretariat.

1.3.3 The ICT Committee Shall:

- i. Provide a forum for the continuous evaluation and assessment of existing ICT services and infrastructure;
- ii. Identify and communicate to ICT Department any emerging needs across the university domain areas;
- iii. Act as Change Agents during the introduction of new innovation or new ICT services and
- iv. Act as the link for the university-wide user community engagement with ICT Department as regards the ICT Service Provision.

1.3.4 Heads of Teaching, Learning, Administration and Research Units shall:

- i. The Principals/ Heads of Departments shall in consultation with the ICT Department, integrate ICTs into their activities, implement the Unit specific components of the ICT Policy and Strategy, ensure compliance to the ICT Policy Framework.
- ii. Act as active participants during the periodic stakeholder consultations towards supporting and facilitating the effective implementation of the ICT Policy and Strategy.

1.3.5 The Staff, Student Community and Guest Users shall ensure compliance to the ICT Policies.

**1.4 Enterprise Architecture Principle**

1.4.1 Enterprise Architecture is a business strategy which documents, classifies, analyses and captures all aspects of the university's digital environment. The Enterprise Architecture belongs to the University Executive, this is so as it has to be 100% aligned to the University Strategic Plan and goals. The Directorate of ICT must conform to an enterprise architecture framework and principles that augment the digital capabilities of the university as part of ICT governance.

1.4.2 The principles of enterprise architecture will guide the design, selection, and implementation of ICT solutions in terms of information, applications and technology.

1.4.3 The ICT Department shall establish a criteria for the selection of ICT infrastructure or technologies.

1.4.4 The ICT Department shall define the functional requirements of the Enterprise Architecture;

1.4.5 The ICT Department shall assess existing ICT infrastructure and future ICT technologies, for compliance with technology standards and its support of the university's business processes.

1.4.6 Information, Application and Technology Architecture Principles are as follows:

- i. Information is a very critical and valued corporate resource and must be managed accordingly.
- ii. Data must be accessible and shared for users to perform their tasks.
- iii. Information must be protected from unauthorised access, unauthorised use and disclosure.
- iv. Applications should operate on a variety of technology platforms.
- v. Applications must be easy to use so that users can perform their tasks smoothly.
- vi. Changes to technology and applications must be made in response to evolving technologies and business requirements.
- vii. Hardware and software must conform to defined standards that promote interoperability for applications, data and technology.
- viii. Changes to the university's information operating environment must be planned and implemented in a timely manner.

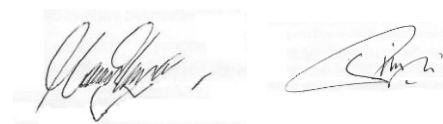
**1.5 Third Party Management**

- 1.5.1 A third party is a supplier or service provider who is external to Chinhoyi University of Technology (CUT) and provides products and/or services that contribute to the overall service provided to CUT staff and students. There must be a service agreement between CUT and all its third party service providers as part of ICT governance best practice.
- 1.5.2 Service Level Agreements (SLAs) must conform to the following areas:
- i. Duration- This is the period of the contract. The service provider outlines the time frame of service being provided given the nature of the service. CUT may specify the period it needs the service.
  - ii. Fees and Charges-The service provider and Chinhoyi University of Technology must explicitly agree on the terms and conditions of payment for the service(s).
  - iii. Definition of Responsibility-The Registrar is responsible for signing the contract. The ICT Department through the ICT Director is responsible for liaising with the service providers to get the best possible service(s).
- 1.5.3 Service providers have the responsibilities of meeting response times associated with service related incidents and provide appropriate notification to customers for all scheduled maintenance.
- 1.5.4 Each party agrees to comply with safety and security procedures notified to them by the other party.

- 1.5.5 The service provider must meet all required delivery dates as per agreement unless there is a challenge, which must be clearly communicated.
- 1.5.6 The Service provider and Chinhoyi University of Technology must agree on the terms and conditions of service and what happens in case of a breach.
- 1.5.7 Either party may terminate a service at the end of an initial Term or Renewal Term by providing the other party normally with at least one (1) calendar month written notice.
- 1.5.8 Either party may terminate the contract once all services have expired or been terminated, by providing the other party normally with at least one (1) calendar month written notice.
- 1.5.9 In the event of any dispute arising between the parties under the SLA, the parties will act in good faith to attempt to settle the dispute through discussions between senior representatives, CEO's or equivalent office bearers. Discussions will normally be held within one (1) calendar month of a party giving the other party notice of the issue in dispute.
- 1.5.10 In determining any dispute between the parties by arbitration, the law of Zimbabwe shall normally be applicable.

## **1.6 Project Management.**

- 1.6.1 Project management is the planning and organization of resources in order to accomplish a specific task or a set of tasks to satisfy business requirements. Project management normally involves once off tasks different from daily routine activities.
- 1.6.2 The ICT management must come up with a detailed project plan for all projects to be carried out. The project plan must state the following:
  - i. A detailed list of resources required that is labour, materials, and the cost of materials.
  - ii. Project completion time frame and list of tasks to be performed (Gantt chart).
  - iii. Risks that may have a direct impact on the project outcome.
  - iv. Roles and responsibilities that each and every person involved in a project must be given a specific task(s) that he/she is accountable for.
- 1.6.3 There must be a clearly laid out project reporting structure.
- 1.6.4 The project should be monitored on a regular basis in terms of time, cost and quality of the project outcome.
- 1.6.5 At the end of each project, the project leader must compile a report and forward it to ICT management. The project report should cover the following items:
  - i. Name of the project.



- ii. Resources used
- iii. Project status - was the project completed on time and on budget?
- iv. Risks – point out identified risks and controls.
- v. Recommendations for future projects.

## **1.7 Audit and Compliance**

- 1.7.1 Audit provides independent, objective assurance and advisory activity designed to add value and improve university operations. It helps the university accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.
- 1.7.2 Compliance provides oversight of the institutional compliance program and the distributed processes that support compliance across the university.
- 1.7.3 The primary purpose of internal audit is to add value to the university's operations by providing an independent appraisal and advisory function for ICT Committee and ICT Department thereby assisting the university in realizing its corporate goals. This is achieved by examining and evaluating the adequacy, effectiveness and efficiency of ICT controls.
- 1.7.4 A review or appraisal by internal audit does not in any way relieve ICT officers of the university of their individual responsibilities and accountability. Nor does it in any way diminish the Vice-Chancellor, and other executive management's responsibilities for the implementation and maintenance of effective ICT systems of internal control and prevention and detection of intrusions.
- 1.7.5 The university and its consolidated entities are required to have an external audit of statutory compliance
- 1.7.6 External Audit must be given full, free and unrestricted access to any and all records, physical properties, personnel and other documentation belonging to, in the custody of, or under the control of, the university. All employees are to assist External Audit in fulfilling its roles and responsibilities.
- 1.7.7 It is the responsibility of External Audit to audit the annual ICT performance and prepare an auditor's report in accordance with audit professional guidelines. The external auditor shall present findings report and recommendations to the university's management just as is the case with the financial audit of the university

---

## **2. ICT SERVICE MANAGEMENT POLICY**

---

### **2.1 Introduction**

- 2.1.1 The university shall ensure the provision of ICT Services within the university, and as well as define the ICT Department as the central coordination point for all ICT support.
- 2.1.2 The ICT support shall cater for all areas under the university network, computing devices, hardware, software and implementation of ICT initiatives, projects and programs at all campuses and their related support services.

### **2.2 Policy Objective**

- 2.2.1 To define and implement an effective ICT Service Management and Support approach that is aligned to the university's Strategic Plan where ICT is identified as a key enabler of the university's strategic vision.
- 2.2.2 To provide for the integrated management, responsibility and support of all ICT related matters within the university and its affiliates.

### **2.3 Roles and Responsibilities**

- 2.3.1 The university shall define and implement an appropriate ICT Service Management process and procedure aligned to the goals and objectives of the university. The ICT Department shall define and implement a Business Model for the provision of ICT services to internal and external clientele.
- 2.3.2 The ICT Help Desk will act as the central point of contact for all ICT support requests. The ICT Department shall formulate and implement relevant standard operating procedures (SOP) to set service quality and time delivery standards for all services it provides to its user community.

#### **2.3.3 ICT Services Support & Help desk**

The ICT Services Support will be defined as such operations carried out by authorized personnel to ensure efficiency, stability and continuity of any ICT service or equipment to ensure it meets its intended user requirements.

#### **2.3.4 ICT Services Support Personnel**

The ICT Services personnel employed by the Chinhoyi University of Technology within all departments and schools shall functionally report to the ICT Department. The university shall provide the necessary work tools, safety wear and training for all ICT services support personnel.

Accordingly, such personnel shall:

- i. Ensure protection mechanisms exist against ICT devices tampering, alteration or theft;
- ii. Ensure ICT protection controls exist to safeguard security of systems and information;
- iii. Provide assistance and guidance towards compliance to ICT policies.
- iv. Provide technical support in line with approved ICT standard operating procedures for any system, service, device downtime or breach;
- v. Ensure installation and configuration of all hardware and software is aligned to approved ICT standards;
- vi. Ensure safe custody and authorized usage of all university software licences, copyright, usage keys and backups.

## **2.4 ICT Maintenance**

### **2.4.1 The ICT Department shall:**

- i. From time to time define and disseminate updated ICT equipment maintenance guidelines to all university administrative and academic units.
- ii. Act as the central point of contact for all university ICT equipment maintenance
- iii. Provide technical support in the development and implementation of service and maintenance schedules for all university ICT equipment
- iv. Undertake a periodic assessment in university administrative and academic units to ensure compliance with the set maintenance guidelines

### **2.4.2 Departments, Institutes, Directorates and Schools within the university shall:**

- i. Maintain records of all ICT equipment they acquire including records of manufacturer equipment warranty
- ii. Liaise with the ICT Department in developing service and maintenance schedules on an annual basis for all ICT equipment
- iii. Maintain good documentation describing the service and maintenance history for all ICT equipment
- iv. Ensure all ICT equipment is placed within adequate operating environments
- v. Ensure all replacements or upgrades of any ICT equipment is undertaken with clearance from the ICT Department.

## **2.5 ICT Skills and Capacity Building**

The adoption of Information and Communications Technology (ICT) products and tools will require personnel training to enable effective usage. This requires a dedicated approach within the university to be able to plan for such gaps and develop



as well as implement the training as need arises. This will target all users (both students and staff) within the university.

## **2.6 ICT Capacity Building Assessment**

The ICT Department in partnership with Human Resources Department and Heads of Departments shall coordinate periodic assessment of existing ICT skills capacity amongst all user groups to be able to identify gaps. The ICT Department shall also undertake a periodic capacity skills assessment to identify knowledge gaps within its technical staff to be able to seek appropriate capacity building programs.

## **2.7 ICT Capacity building delivery methods**

The ICT Department shall develop capacity building modules and courseware for identified ICT skills gaps, and implement such courseware with either internal resource personnel or with external subject matter experts as per the nature of the required training. The university through the guidance of the ICT Department shall also insure the presence of well-equipped ICT training computer labs.

---

### **3. GENERAL ICT INFRASTRUCTURE USE POLICY**

---

#### **3.1 Introduction**

- 3.1.1 This policy is intended to protect the university's employees, students and guest users as well as the university from the consequences of illegal or damaging actions by individuals using the university ICT resources.

#### **3.2 Policy Objective**

- 3.2.1 To define the acceptable use of the university ICT resources and protect the university and authorized users from risks including service unavailability, legal liability, malware attacks, and the compromise of network systems, services and information.

#### **3.3 Access to ICT Facilities**

- 3.3.1 The university provides computer facilities and access to its computer networks only for purposes directly connected with the work of the university and with the normal academic activities of their members.
- 3.3.2 Individuals may make use of university ICT facilities only with appropriate authorisation.
- 3.3.3 'Appropriate authorisation' in this context means by virtue of being a registered CUT student, staff or prior authorisation by the appropriate officer, who shall be the ICT Director or any officer acting on his/her behalf.
- 3.3.4 Any authorisation is subject to compliance with the university's statutes and regulations, including the ICT policy, and will be considered to be terminated by any breach or attempted breach of these regulations.
- 3.3.5 Authorisation will be specific to an individual.
- 3.3.6 Any password, authorisation code, etc. given to a user will be for his or her use only, and must be kept secure and not disclosed to or used by any other individual.
- 3.3.7 Exceptions may be made for accounts set up specifically to carry out business functions of the university or a unit within it. A written authorisation must be given by the head of the respective unit.

### **3.4 Acceptable Use**

- 3.4.1 University ICT facilities are provided for use in accordance with the following regulations as set and/or approved by the University Council.
- 3.4.2 Data created by authorized users is property of the university.
- 3.4.3 The university reserves the right to audit networks and systems on a periodic basis and ad hoc when need arises to ensure compliance with the university Information and Communication Technology Policies.
- 3.4.4 Authorised users are required to take all necessary steps to prevent unauthorized access to sensitive information.
- 3.4.5 Authorized users are responsible for logging out of all systems and accounts when they are not being used; system sessions must not be left unattended.
- 3.4.6 Authorised users must switch off all university computers after use as a way of saving power and securing systems from unauthorised access.
- 3.4.7 All laptops and workstations are required to be secured with a password and users must log-off when the device is unattended.
- 3.4.8 All computers used by authorized users that are connected to the university Information and Communication Technology network, whether privately owned by the individual or the university, must be continually executing approved virus-scanning software with a current virus database.
- 3.4.9 Authorized users must avoid opening email attachments received from unknown senders/sources, which may contain viruses, email bombs or Trojan horse codes or any other malicious software.

### **3.5 Unacceptable Use**

- 3.5.1 Any unlawful activity; creation, transmission, storage, display or downloading, of any obscene, offensive, indecent, or menacing images, data, or other material, or any data capable of being resolved into such images or material, except in the case of the use of the facilities for properly supervised research purposes when that use is lawful and when the user has obtained prior written authority for the particular activity as approved by the ICT Director.
- 3.5.2 The creation, transmission, or display of material which is designed or likely to harass another individual in breach of national laws on harassment.
- 3.5.3 The creation or transmission of defamatory material about any individual or organization.

- 3.5.4 The sending of any email that does not correctly identify the sender of that e-mail or any message appearing to originate from another individual, or otherwise attempting to impersonate another individual.
- 3.5.5 Sending any message that attempts to disguise the identity of the computer from which it was sent.
- 3.5.6 Transmission, without authorisation of Email to a large number of recipients, unless those recipients have indicated an interest in receiving such e-mail, or the sending or forwarding of Email which is intended to encourage the propagation of copies of itself.
- 3.5.7 Creation or transmission of or access to material in such a way as to infringe a copyright, moral right, trade mark, or other intellectual property right.
- 3.5.8 Private profit, except to the extent authorised under the user's conditions of employment or other agreement with the university or a school; or commercial purposes without specific authorisation.
- 3.5.9 Gaining or attempting to gain unauthorised access to any facility or service within or outside the university, or making any attempt to disrupt or impair such a service.
- 3.5.10 Activities not directly connected with employment, study, or research in the university or the school's (excluding reasonable and limited use for social and recreational purposes where not in breach of these regulations or otherwise forbidden) without proper authorisation.
- 3.5.11 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted Software for which the university or the authorized user does not have an active license is strictly prohibited.
- 3.5.12 Introduction of malicious software into the university Information and Communication Technology resources (e.g., Viruses, Worms, Trojan Horses, e-mail bombs, etc.).
- 3.5.13 Revealing or sharing account password with others or allowing use of an authorized user's account by others, including family and other household members.
- 3.5.14 Using someone's credentials to gain access to any university system.
- 3.5.15 Making fraudulent offers of products or services originating from any university account or otherwise made from a computer connected to the university's information and communication technology network and resources.
- 3.5.16 Port scanning or security scanning is expressly prohibited unless explicitly authorized by the ICT Director.

- 3.5.17 Executing any form of network monitoring or scanning, unless this activity is a part of the authorized user's normal job/duty.
- 3.5.18 Circumventing user authentication or security of any device, network, or account.
- 3.5.19 Using virtual private networks or proxies to circumvent predefined restrictions.
- 3.5.20 Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, by any means locally or remotely.
- 3.5.21 Providing unauthorised information about, or lists of, university employees or students to non-university parties.
- 3.5.22 Offering commercial services through systems connected to the university network, or to provide other ICT facilities for any commercial organization, except with the permission of the University Executive through the ICT Director.
- 3.5.23 Use of file-sharing technology and participation in distributed file-sharing networks is subject to additional regulation and restriction and should be authorised by the ICT Director.

### **3.6 Termination and or Suspension of User Access**

- 3.6.1 The following constitute rationale for user access termination to university computing resources:
  - i. End of student or staff employment tenure
  - ii. Request, in writing, from University Council, University Management, Heads of Department and/ or university human resource department
  - iii. Occurrence of any of the unacceptable usage restrictions

### **3.7 Bring Your Own Device (BYOD)**

- 3.7.1 The university shall allow the usage of personal devices on the university network as long as such complies with the university policies and offers a similar level of protection as specified by the ICT Department.
- 3.7.2 Such usage will be subject to the following:
  - i. Registration of BYOD capabilities and device profiles with both the ICT Department and the Campus Protection Service.
  - ii. Agreeing to provide the ICT Department and the Campus Protection Service (CPS) limited authority over the device for the sole purpose of protecting university data and access on the device for the purpose of investigation.
  - iii. The device has an updated/current antivirus solution.

- iv. Accepting responsibility for ensuring that the personal device is adequately secured against loss, theft or use by persons not authorised to use the device.
- v. No sensitive or confidential university information shall be stored on such devices.
- vi. The owner is responsible for replacing, maintaining and arranging technical support for their device.
- vii. The university will only provide best efforts support for any applications that the university has provided and for network connection troubleshooting.

### **3.8 Control over user activities**

- 3.8.1 The university reserves the right to exercise control over all activities employing its computer facilities, including examining the content of users' data, such as e-mail, where necessary, for the proper regulation of the university's facilities.
- 3.8.2 User activity check might be in connection with properly authorised investigations in relation to breaches or alleged breaches of provisions in the university's statutes and regulations, including these regulations; or
- 3.8.3 To meet legal requirements or otherwise in the context of legal proceedings or the taking of legal advice, in accordance with such procedures as may be approved by the University Council for this purpose.

---

## 4. DATA PROTECTION & CLASSIFICATION POLICY

---

### 4.1 Introduction

- 4.1.1 A data protection and classification policy is necessary to provide a framework for securing data from risks including, but not limited to, creation, unauthorized destruction, modification, disclosure, access, use, and removal.
- 4.1.2 This policy outlines measures and responsibilities required for securing data resources. It shall be carried out in conformity with national laws (*Data Protection Act [Chapter 11:12]*).

### 4.2 Policy Objective

- 4.2.1 To provide a framework for securing data from risks including but not limited to, create, unauthorized destruction, modification, disclosure, access, use, and disposal or removal.

### 4.3 Data Classification

- 4.3.1 The ICT Department shall ensure that data at all levels is maintained in a secure, accurate, and reliable manner and be readily available for authorized use.
- 4.3.2 To implement security at the appropriate level, establish guidelines for legal/regulatory compliance, and reduce or eliminate conflicting standards and controls over data, data shall be classified into one of the following categories, **confidential data, restricted data and public data**

#### 4.3.3 Confidential Data

Data is classified as Confidential when an unauthorized disclosure, alteration or destruction of that data will cause a significant level of risk to the university. Access to confidential data must be individually requested and then authorized by the data owner who is responsible for the data. The assessment of risk and access approval will be determined by the data owner or risk committee.

#### 4.3.4 Restricted Data

Sensitive information that would not necessarily expose the university to significant loss, or threat but the data owner has determined security measures are needed to protect from unauthorized access, modifications, or disclosure. This also includes all internal information assets that are not explicitly classified as confidential data but requires a reasonable level of security controls.

#### 4.3.5 Public Data

Data will be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in no risk to the university and its affiliates.

#### 4.4 Data Classification Diagram

	Public Data	Restricted	Confidential
Example	<p>Directory/contact information not designated by the owner as private.</p> <p>Name</p> <p>Addresses (campus and home)</p> <p>Email address</p> <p>Listed telephone number(s)</p> <p>Degrees, honours and awards</p> <p>Most recent previous educational institution attended</p> <p>Major field of study</p> <p>Dates of current employment, position(s)</p> <p>Class year</p> <p>Participation in campus activities and sports</p> <p>Weight and height (athletics)</p> <p>Dates of attendance</p> <p>Status</p> <p>Business Data</p> <p>Campus maps</p> <p>Job postings</p> <p>List of publications (published research)</p> <p>Brochures/flyers</p>	<p>Personal/Employee/Student Data</p> <p>Student ID number</p> <p>Payroll information</p> <p>Personnel records, performance reviews</p> <p>Race, ethnicity, nationality, gender</p> <p>Date and place of birth</p> <p>Directory/contact information designated by the owner as private</p> <p>Business/Financial Data</p> <p>Financial transactions which do not include confidential data</p> <p>Information covered by non-disclosure agreements</p> <p>Contracts that don't contain Personally Identifiable Information (PII)</p> <p>Credit reports</p> <p>Records on spending, borrowing, net worth.</p> <p>Academic / Research Information</p> <p>Library transactions</p> <p>Unpublished research or research detail / results that are not confidential data</p> <p>Private funding information</p> <p>Course evaluations</p> <p>Systems/Log Data university</p> <p>Systems/Server event logs.</p>	<p>Personally Identifiable Information (PII):</p> <p>Social Security Number (SSN)</p> <p>Driver's license</p> <p>State ID card</p> <p>Passport number</p> <p>Financial account, credit card, or debit card numbers</p> <p>Protected Health Information:</p> <p>Health status</p> <p>Healthcare treatment</p> <p>Healthcare payment</p> <p>Student Data:</p> <p>Loan or scholarship information</p> <p>Payment history</p> <p>Student tuition bills</p> <p>Student financial services information</p> <p>Class lists or enrolment information</p> <p>Transcripts; grade reports</p> <p>Notes on class work</p> <p>Disciplinary action</p> <p>Business /Financial Data</p> <p>Passwords to all university database systems.</p>
Storage	<p>No other protection is required for public information; however, care should always be taken to use all university information appropriately.</p>	<p>Level of required protection of Restricted data is either pursuant to CUT policy or at the discretion of the data or information owner. If appropriate level of protection is not known, check with the ICT Department before storing restricted data unencrypted.</p>	<p>Confidential data should only be stored on university-administered servers or the university's approved cloud storage systems and must not be store on personal computers or PDAs. Confidential data that will be stored by a vendor or application hosting provider must be protected and secured to the same</p>



			standards applied by the university.
Transmission	No other protection is required for public information; however, care should always be taken to use all university information appropriately.	Transmission through any electronic messaging system (e-mail, instant messaging, text messaging), is also strongly discouraged.	Transmission through any electronic messaging system (non-university email, instant messaging, text messaging) is strictly prohibited. Confidential data sent or received electronically can be transmitted using the university's email system. In addition, protected data can be transmitted using secure web transfer, or the Secure File Transfer Protocol. Other acceptable methods include transferring files between network drives on the university's internal network or using the university's secure web file system
Disposal	Electronic information should be deleted using normal file deletion processes in accordance with any retention schedule. Printed copy should be disposed of via the university paper recycling scheme and in accordance with any retention schedule.	Electronic equipment holding this information must be disposed of using the university secure IT waste disposal service and in accordance with any retention schedule. Printed copy should be disposed of via the university confidential waste scheme and in accordance with any retention schedule.	Electronic equipment holding this information must be disposed of using the university secure IT waste disposal service and in accordance with any retention schedule. Printed copy should be disposed of in accordance with any retention schedule via the university confidential waste scheme or departmental shredding facilities. Large accumulations of data should not be downloaded or copied.

---

## **5. CLOUD COMPUTING POLICY**

---

### **5.1 Introduction**

- 5.1.1 This policy codifies an enabling framework to manage the way the university accesses and uses cloud services, while avoiding a 'shadow IT' environment.

### **5.2 Policy Objective**

- 5.2.1 To ensure Chinhoyi University of Technology's commitment to all its legal, ethical and policy compliance requirements are met in the procurement, evaluation and use of cloud services.

### **5.3 Cloud Computing Definition**

- 5.3.1 'The Cloud' is shorthand for the provision of computing services that are accessed via the internet. For this reason, they are readily accessible and can also be scaled up or down as required. Their use though, is not without risk. Adopting a service from "the cloud", particularly a business system, may not be any less challenging to implement than an in-house service, and indeed may expose users to unanticipated risks, costs and/or service outages.

- 5.3.2 To address these risks and accommodate the requirements of different user communities across campus, this document establishes the university's position on selection, use and business rules surrounding the use of cloud services.

### **5.4 Cloud Management Framework**

- 5.4.1 The cloud management framework applies to the university as a whole, but recognizes that different university functions have different requirements.
- 5.4.2 This policy codifies a cloud selection and management framework that sets out the university's approach to cloud use and adoption, and integrates this with existing university information management policies;

### **5.5 Cloud Risk Management**

- 5.5.1 Cloud services must be chosen, implemented and used with reference to the university's risk management models and frameworks.
- 5.5.2 Risk assessments will be right sized and appropriate to service type and the information type.

### **5.6 Compliance Assurance**

- 5.6.1 Cloud services must be able to comply with the university's legal obligations, and must enable the repatriation of content to the university to allow legal obligations to be fulfilled.

## **5.7 Cloud Registration and Management**

- 5.7.1 All cloud services must be centrally requested and registered following the cloud registration and approval procedures to enable the management of their content and contractual terms and conditions, and to ensure they meet the national and university's security, access and non-functional requirements for ICT systems.
- 5.7.2 The ICT Directory shall develop a standard operation procedure (SOP) for cloud service registration and management.

## **5.8 Cloud Usage**

- 5.8.1 All cloud services commissioned under this policy and the content they create and maintain, are university services and must be used appropriately and in line with other university policies and procedures, including security and access.
- 5.8.2 Although not located within the university, cloud services are nevertheless IT services and must be considered within that context.

## **5.9 Recognition of Cloud Service Limitations**

- 5.9.1 Many Cloud service providers, particularly those that offer Software as a Service (SaaS) may use proprietary and/or highly controlled data/software formats. These often do not have export capabilities that enable the continued processing or editing of the content on a different platform.
- 5.9.2 When considering cloud services these limitations should be taken into account and assessed. They will be considered during the review and approval process. Decision making factors will include, but are not limited to, the information value level of the content proposed to be created/stored in the service, its IP value and whether it contains personal or sensitive personal information.

---

## **6. DATA COMMUNICATIONS NETWORK POLICY**

---

### **6.1 Introduction**

- 6.1.1 This Policy sets out to achieve a rationalized infrastructure approach that will lead to the emergence of centralized network management through the Network Operations Center.
- 6.1.2 This does require an appropriate policy to guide the development, maintenance and usage of the university network backbone.

### **6.2 Policy Objectives**

- 6.2.1 To guide the development, rollout, maintenance and usage of the university network backbone to ensure resiliency, stability and higher uptime rates.
- 6.2.2 To ensure the usage of the backbone is aligned to the goals of the university as laid out in the university Strategic Plan.

### **6.3 Communication Network Infrastructure**

- 6.3.1 The university shall provide a resilient, secured and stable fast data communications network as an enabler to the processing, storage, dissemination and accessing of information or ICT enabled services as relates to the various needs of the teaching, learning, administration, research, innovation, and industrialization domains.
- 6.3.2 The ICT Department, shall develop and maintain an updated university-wide enterprise architecture as the blueprint for alignment of business requirements and ICT investments;
- 6.3.3 All new network expansions shall be approved by ICT Department to ensure alignment to the existing network design;
- 6.3.4 The university shall establish and maintain a Data Center/Server Room to act as the central repository for all university databases, networking systems and web hosting;
- 6.3.5 Introduction of new technology within the network management or provision shall undergo professional testing to ensure compliance with existing standards and performance requirements;
- 6.3.6 Heads of Departments will at each annual budgeting cycle plan for its specific ICT requirements for proper provisioning in a rationalized manner; and
- 6.3.7 The university shall develop and maintain updated structured cabling standards to ensure a uniform level of acceptable design and access across all units.

#### **6.4 Digital Network**

- 6.4.1 The university digital network will be defined as all such equipment involved in the transmission and routing of all digital communications within the university at all campuses.
- 6.4.2 The management of the entire digital network infrastructure shall be vested with the ICT Department.
- 6.4.3 The ICT Department shall periodically define the methodology for access to internal and external data destinations and data routes;
- 6.4.4 The university shall establish central monitoring and control of the university-wide digital network
- 6.4.5 All Domain Name Services (DNS) activities hosted within the university shall be centrally managed;
- 6.4.6 All core network components shall be designed to support redundancy for continued service provision;

#### **6.5 University Wide Area Network**

- 6.5.1 The university Wide Area Network (WAN) refers to all the aggregated inter-connected campuses on the virtual one-network university domain.
- 6.5.2 All the external university campuses shall be interlinked onto the main campus network through Virtual Private Network (VPN) connection.
- 6.5.3 The ICT Department shall be responsible for management of all WAN links and networks.
- 6.5.4 The computer network within each external campus shall form a campus Local Area Network (LAN) and will have a designated technical personnel under the supervision of the ICT Department.
- 6.5.5 The university shall provide a secure and resilient university LAN.
- 6.5.6 All campus LANs will ensure compliance with approved university ICT structured cabling standards and network configurations

#### **6.6 Wireless Access Provision**

- 6.6.1 This refers to the provision of connectivity to the internet using wireless technology through authorized access points.
- 6.6.2 The university will support the provision of reliable and secured near-ubiquitous Wireless Access Points across the university campuses;
- 6.6.3 The ICT Department will approve wireless access points to be installed and transmit wireless signals from time to time.

6.6.4 The configuration of such Wireless Access Points shall comply with approved network and security configurations to achieve consistency and performance standards;

6.6.5 The Wireless Access health monitoring and technical support shall be the responsibility of the ICT Department.

## **6.7 Remote Access**

6.7.1 The university will support the provision of remote access for approved university resources. This supports the provision of access to network resources to authorized users across public internet infrastructure with consideration for information security.

6.7.2 The ICT Department shall define and implement the remote access methodology, technology and standard as the requirements to ensure privacy and security.

6.7.3 Remote Access shall only be provided to users approved by the ICT Director, as justified by Heads of Departments, as per the business need requirement.

6.7.4 All approved users for the remote access functionality shall consent to the ICT policy.

6.7.5 An authorised user bear's responsibility for the consequences should this access be misused.

6.7.6 Authorised users with remote access privileges must ensure that their connected devices do not connect to other devices at the same time.

6.7.7 The ICT Department shall be responsible for remote access usage monitoring and control, and shall develop specific standard operating procedures for remote access.

## **6.8 Access to Network Infrastructure and ICT Services**

6.8.1 Access to university Data Centre/Server Rooms and other network equipment installations shall be secured and only allowed to authorised personnel.

6.8.2 Movement of any network equipment and/or installation shall be only as authorized by the ICT Director.

6.8.3 The ICT Department shall maintain an updated Network Equipment asset register.

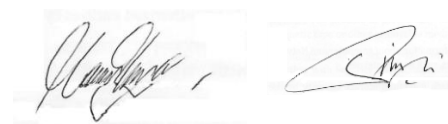
6.8.4 All ICT equipment to be installed onto the university network shall comply with approved university specifications as spelt out by the ICT Director from time to time.

6.8.5 All installations or modifications of any network equipment shall be approved and supervised by the ICT Director.

6.8.6 The ICT Director shall define and manage all Service Level Agreements (SLA) with third party service providers for bandwidth provision and any other ICT related service.

- 6.8.7 All external third party connections to the university network shall comply with the university ICT Policies;
- 6.8.8 All contractors or third party access to any server room or network equipment installation shall be authorized and supervised by the ICT Director.

i.

Two handwritten signatures in black ink, one on the left and one on the right, both appearing to be in cursive script.

---

## **7. SOFTWARE DEVELOPMENT POLICY**

---

### **7.1 Introduction**

- 7.1.1 In order to be successful, all software development application projects must undergo a well-defined development lifecycle.
- 7.1.2 This policy establishes the minimum requirements and responsibilities for such a lifecycle of all systems to be developed at Chinhoyi University of Technology under the ICT Department.

### **7.2 Policy Objective**

- 7.2.1 To define and implement software development and acquisition methodology to increase efficiency, information assurance, value for university resources and enhance rationalization of ICT.

### **7.3 Software Development System Life Cycle**

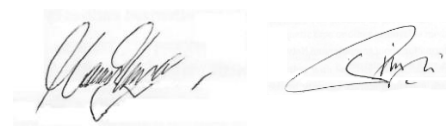
- 7.3.1 The ICT Department shall periodically define the Systems Development Cycle methodology for, information classification, usage of the least privilege principle, segregation of roles and audit trails.
- 7.3.2 All software shall undergo thorough testing and quality assurance before installation in any production environment within the university.
- 7.3.3 All software under this policy shall comply with the Software Licensing and Ownership and Cyber Security Policy.
- 7.3.4 All acquired software shall where necessary contain provision for technical support and upgrades.
- 7.3.5 All university campuses, schools, 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.

### **7.4 Secure Software Development**

- 7.4.1 Each programmer is responsible for implementing this policy when developing any given system at any given time.
- 7.4.2 Agile development shall be followed and implemented in the development of any application.
- 7.4.3 Terms of reference and feasibility shall be agreed and signed by all relevant parties before the development of any application and or updating. This refers to both in-house developed and off-the-shelf software.



- 7.4.4 Thorough and complete documentation (Business Case, User Manual and Technical Manual) shall be produced for every in-house developed software.
- 7.4.5 Each module shall be tested for functionality and security before being passed as correct (i.e. is the module doing the right thing). A development, test, and production server shall be maintained.
- 7.4.6 Each version of the developed application shall be backed up and logged into the backup log book before being uploaded to the server.
- 7.4.7 Source code of every developed application shall be backed up and stored at the backup server and or offsite backup.
- 7.4.8 Every module that reads from and or records data into the database shall have user logs for future reviews.
- 7.4.9 The ICT Department shall develop a SOP for software development.



---

## **8. CHANGE MANAGEMENT POLICY**

---

### **8.1 Introduction**

- 8.1.1 This policy describes a systematic process to document and manage changes to the university Information and Communication Technology Network and software in order to permit effective planning by the university ICT to serve the university user-base.

### **8.2 Policy Objectives;**

- 8.2.1 To guide the management of changes to the ICT infrastructure to enable ICT Department staff members and stakeholders to plan accordingly, so as to reduce the impact of changes on other tasks/projects.
- 8.2.2 To promote communication and collaboration regarding change items.
- 8.2.3 To maintain compliance to applicable regulations.

### **8.3 Change Management Procedure**

- 8.3.1 Any change to a university ICT infrastructure is subject to this policy, and must be performed in compliance with these procedures.
- 8.3.2 All changes affecting university ICT infrastructure must be reported to or coordinated with the ICT department.
- 8.3.3 A formal written change request must be submitted to the ICT Department for minor, emergency, and major change categories, both scheduled and unscheduled.
- 8.3.4 The ICT Director shall appoint a five (5) member Change Management Committee (CMC) from the staff members, to manage the change process. The ICT director shall chair the Change Management Committee and appoint two (2) members on request basis from the change requesting department/section to attend CMC meeting.
- 8.3.5 To ensure successful review, approval, implementation and closure of change items, each core ICT service area and change requester/initiator should be represented during the Change Management Meeting.
- 8.3.6 All scheduled change requests and supportive documentation must be submitted to the CMC in compliance with the Change Management Procedure.

### **8.4 Approval & Deferral of Change**

- 8.4.1 The Change requester needs to submit a formal written Change Request to the ICT department through the ICT Helpdesk.

- 8.4.2 Changes that impact the entire university will require pre-communication through established electronic media like email and website. Changes that impact specific sections of the university should be communicated accordingly to the affected sections.
- 8.4.3 Once a change request is submitted it will be known as a change item and is assigned a change number.
- 8.4.4 The sectional manager responsible for the change item shall assign a change category upon receiving the change request and action based on the approval requirement of the change.
- 8.4.5 Authorization of a change item occurs after the change is reviewed and depends on the priority of the item as described in the table below.

<b>Change Category</b>	<b>Description</b>	<b>Approval</b>	<b>Change Request Document</b>
Standard	This type of change is performed on a regular basis and is considered routine.	Not Required	Not Required
Minor	Small changes or changes that have a small or minor effect.	Sectional Manager.	Required
Emergency	This type of change is usually a response to a failure or error that needs an urgent fix and may fall under minor or major. Emergency changes must be made quickly and are usually recorded after the change has already been made.	Post change review by the CMC	Required
Major	This type of change requires a lot of items or dependencies and may require other associated change requests.	CMC	Required

- 8.4.6 If the change is approved, it is then assigned to the respective sectional manager to action the request.
- 8.4.7 All changes shall be logged and documented, capturing the scope of the change, areas affected, back-out process, testing completed, communication plan and planned date of deployment.
- 8.4.8 Emergency, Minor and Major changes shall first be implemented on a development platform.
- 8.4.9 All changes shall conform to the cybersecurity checklist.

## **8.5 Closing a Change Request**

- 8.5.1 Change items that are previously approved and subsequently deployed are reviewed for closure during the Change Management Committee meetings.
- 8.5.2 The change requester or an informed representative should be available at the change meeting to discuss the implementation.
- 8.5.3 The review should note the status of the change item execution and any service or infrastructure impacts. If the change has performed as desired it may be closed.
- 8.5.4 In the event a change does not perform as expected or causes issues to one or more areas of the production environment, the attendees of the change meeting will determine if the change should be removed and the production environment be restored to its prior stable state.
- 8.5.5 Appropriate action should be noted within the change application and successfully acted upon prior to marking the item closed.
- 8.5.6 The ICT Department shall develop Change Management SOP.

---

## **9. CYBER SECURITY POLICY**

---

### **9.1 Introduction**

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

### **9.2 Policy Objectives**

- 9.2.1 To ensure the security of ICT services and facilities, information assets and associated infrastructure, so as to minimize the exposure of the Chinhoyi University of Technology to Cyber Security risks.
- 9.2.2 To create awareness across Chinhoyi University of Technology on the appropriate security measures must be implemented as part of the effective operation and support of information systems.

### **9.3 Roles and Responsibilities**

9.3.1 The ICT Department shall:

- i. Put in place appropriate security controls and mechanisms based on periodic risk assessment;
- ii. Maintain an updated ICT risk register in line with the University Risk Framework.
- iii. Maintain an updated and tested Business Continuity and Disaster Recovery Plan for all critical university digital infrastructure and information assets.
- iv. Implement periodic systems and infrastructure audit.
- v. Develop and implement a patch management plan
- vi. Implement network filtering to protect the network against cyber-threats.
- vii. Manage the controlled and audited usage of ICT system privileges
- viii. Implement monitoring and real time analysis of all ICT network device event security logs with a centralized mechanism.
- ix. Ensure the implementation of appropriate Wireless Access Provision protection mechanisms
- x. Coordinate periodic cyber-security awareness and training
- xi. Install and continuously update appropriate active malware protection on university computers.
- xii. Develop and maintain a handover mechanism for ICT equipment and information during end of staff employment contracts.
- xiii. Secure access to all the university ICT resources

9.3.2 Users shall:

- 3 Ensure compliance to the cyber-security policy

#### 4 Report any cyber-security incident to the ICT Department

### 9.4 Proper Use of ICT Resources

- 9.4.1 All authorized users of Chinhoyi University of Technology's ICT resources are expected to adhere to the acceptable use as highlighted in this policy through the acceptable use policy.
- 9.4.2 Users must use the ICT facilities in a legal and appropriate manner, to protect the personal safety of themselves and their peers and to ask the university ICT staff for advice or assistance in case there exists a problem.
- 9.4.3 Users must ensure the confidentiality of information such as employee personal information, student records, university manuals, materials, financial data, plans, third party records and other relevant information from the initial creation to disposal.
- 9.4.4 Confidential information must never be released, removed from the university premises, copied, transmitted, or in any other way used by the authorized user for any purpose outside the scope of their university employment, nor revealed to non-university employees, without the express written consent of university management.
- 9.4.5 ICT hardware and software infrastructure must be physically protected against theft, fire and other hazards.
- 9.4.6 All staff, students and third party users are responsible for seeking assistance when in doubt about how to interpret a policy and also to report any concern or suspicious activity encountered.
- 9.4.7 Users can only access data and functionality for which they are authorized ("least privileges" approach).
- 9.4.8 Software installation is restricted to approved ICT Department members only.
- 9.4.9 All ICT devices in the network should be configured securely individually as well as protected by a network architecture that secures the perimeter and incorporates segregation of environments.

### 9.5 Password Rules

- 9.5.1 Passwords are essential to cyber security as they are the front line of protection for authorized user accounts. The ICT Department shall be responsible for defining the password strength, ageing and lifecycle specification for all user categories from time to time.

- 9.5.2 The ICT Department shall implement and maintain centralized authentication, authorization, and accounting service mechanism for all network equipment connected to all ICT resources.
- 9.5.3 All default system or hardware passwords shall be changed.
- 9.5.4 All system-level passwords (e.g. the "root" account on UNIX-based Operating Systems, the "enable" functionality of Routers, the Windows "administrator" account, application administration accounts, etc.) must be changed at least twice every year.
- 9.5.5 All user-level passwords (e.g. Email, web, desktop computer, etc.) must be changed at least thrice every year.
- 9.5.6 Authorized user accounts that have system-level privileges granted through group memberships or Programs such as "sudo" or "SU" must have a unique password that is different from all other accounts held by that Authorized User.
- 9.5.7 Passwords must not be included in Email messages, phone conversations, or other forms of electronic communication.
- 9.5.8 All users shall ensure the privacy and security of their passwords.
- 9.5.9 All users shall ensure the confidentiality of their passwords and are not permitted to share user accounts and passwords.
- 9.5.10 All locally development applications shall support password encryption and user role segregation

## **9.6 Password Construction Guidelines**

- 9.6.1 The ICT Department shall implement and maintain unit specific password complexity on all university systems.
- 9.6.2 Software and Application development standards must ensure that no passwords can be stored in clear text or in any easily reversible form.
- 9.6.3 Password setting for university systems must enforce the inclusion of all four character types; Uppercase letters: A-Z, Lowercase letters: a-z, Numbers: 0-9, and Symbols: ~!@#\$%^&\*()\_+={[]|\;:'<,>./
- 9.6.4 Password setting for all user accounts must enforce the inclusion of three of the four character types; Uppercase letters: A-Z, Lowercase letters: a-z, Numbers: 0-9, Symbols: ~!@#\$%^&\*()\_+={[]|\;:'<,>./
- 9.6.5 Remote Access to the Chinhoyi University of Technology ICT Network must be controlled using either one-time password authentication or a public / private key system with a strong Pass-phrase.
- 9.6.6 All of the rules above that apply to passwords also apply to Pass-phrases.

- 9.6.7 If an account or password is suspected to be compromised, the incident must be reported to the ICT department and the password must be changed immediately.

## **9.7 Physical Security of ICT infrastructure**

Chinhoyi University of Technology assets, including systems and media need to be protected against intentional or accidental physical damage. For that, they shall be located in an area with restricted access and protected against environmental hazards.

## **9.8 ICT equipment and resources allocated to departments**

- 9.8.1 Heads of Departments shall ensure that all ICT infrastructure in their respective sections are compliant to ICT approved standard setup and configurations, routinely checked for unauthorized connections and accessed only by authorized staff, students and/ or researchers.
- 9.8.2 Heads of Departments shall ensure all ICT infrastructure in their respective sections are locked down to prevent physical theft of any component, protected against exposure to water leakages, fire and or dust and serviced.

## **9.9 Data Centre/ Server Room Security**

- 9.9.1 The ICT Department shall ensure that Data Centre/ Server Room facilities are, located in secure strong locations away from human or vehicle traffic, fitted with both manual and electronic access control, with CCTV monitoring, protected against physical intrusion and exposure to water, dust, fire power fluctuations, and supported by alternate power supply

## **9.10 Access Control**

- 9.10.1 The ICT Department shall define and periodically review standard operating procedures for access control for different user categories.
- 9.10.2 The ICT Directory implements CCTV for access monitoring of all university ICT resources and configure system logs, unauthorized activity detection mechanisms and intrusion detection systems on all university systems.

## **9.11 Standard Security Configurations for ICT Infrastructure**

- 9.11.1 The ICT Department shall set up standard security configurations for Network equipment (Routers, Switches, Firewalls, and Servers) and Workstations.
- 9.11.2 Such procedures shall include, maximum attempts required to login to a system, measure to be taken by the system if maximum attempt is reached, systems timeout period, password complexity settings and password ageing settings.



## **9.12 Cyber Security Risk Assessment**

- 9.12.1 Cyber security risk assessment is a mandatory activity, which encompasses information gathering, analysis, and determination of cyber security vulnerabilities within the university's hardware and software environment, and Information and Communication Technology (ICT) business practices. This process is achieved through Vulnerability Assessment and Penetration Testing (VAPT).
- 9.12.2 Cyber Security risk assessment is necessary to analyse and mitigate threats to the university's Information and Communication Technology assets, which may come from any source including natural disasters, disgruntled employees, hackers, the Internet, equipment or service malfunction or breakdown.
- 9.12.3 Cyber Security risk assessments shall be conducted on all information systems including applications, servers, networks, and any process or procedure by which these systems are utilized and maintained.

## **9.13 Vulnerability Assessment and Penetration Testing (VAPT)**

- 9.13.1 Appropriate members of the ICT Department are required to conduct audits, consisting of vulnerability assessments and penetration tests, against the university's computing, networking, and information resources.
- 9.13.2 Audits may be conducted to:
- i. Investigate possible cyber-security incidents
  - ii. Ensure conformance to the university's ICT policies, corresponding regulations and SOPs.
  - iii. Ensure that information is only accessible by the individuals who should be able to access it
  - iv. Ensure that information is protected from modification by unauthorized individuals
- 9.13.3 The ICT Department's Cyber Security unit shall periodically conduct internal vulnerability scans at least quarterly and results of these scans will be addressed in accordance with the risk posed to the university.
- 9.13.4 The university shall outsource external VAPT experts for vulnerability assessment and penetration testing (SLAs to be drafted and signed with terms and conditions of service) annually.

## **9.14 Data Integrity Testing**

- 9.14.1 Data integrity relates to the quality of data in the database system and to the level by which users examine data quality, integrity and reliability. Data integrity testing verifies that the data in the database is accurate and functions as expected within a given application.
- 9.14.2 Each section in the ICT Department shall formulate and implement SOPs for data integrity tests. A SOP is going to be developed for each system in the institution.

## **9.15 Cyber Security Incident Management**

- 9.15.1 Cyber Security Incident Management ensures a consistent and effective approach to the management of Cyber security incidents, including the detection, analysis, eradication and communication of cyber security incidents.
- 9.15.2 The ICT Department shall formulate Cyber Security Incident Response Procedures to define procedures to be taken to manage the lifecycle of cyber security incidents within Chinhoyi University of Technology (CUT), from incident recognition to restoring normal operations.
- 9.15.3 The ICT Department shall record and track all ICT end user related problems.
- 9.15.4 The ICT Department shall put in place mechanisms to be used to alert the ICT Department on any security violation, through Emails, chats, text messages etc.
- 9.15.5 The ICT Department shall periodically update and document cyber-security incidents.
- 9.15.6 The ICT Department shall, as is appropriate, communicate with the users in a manner as to curtail cyber security incidents.

---

## **10. BUSINESS CONTINUITY AND DISASTER RECOVERY POLICY**

---

### **10.1 Introduction**

10.1.1 Chinhoyi University of Technology requires adequate protection to be established to assure the continuity and recovery of the university's major business following the loss or disruption of service.

### **10.2 Policy Objectives**

10.2.1 To define acceptable methods for business continuity and disaster recovery planning, leveraging a risk-based analysis in order to prepare for and maintain the continuity of the university's ICT operations in case of the loss of Critical Infrastructure and Application Services.

### **10.3 Business Risk Assessment and Business Impact Analysis**

10.3.1 The ICT Department is responsible for managing Business Risk Assessment and Business Impact Analysis for each Critical Infrastructure and Application Services that is under its area of responsibility.

10.3.2 The assessment identifies and defines the criticality of Key Business Systems and the repositories that contain the relevant and necessary university data for the Critical Infrastructure and Application Services. The assessment also defines and documents the Disaster Recovery Plan.

#### **10.3.3 Critical Infrastructure Services.**

- vi. Internet Service
- vii. Local Area Network (LAN) Connectivity
- viii. Authentication and authorization systems (*Active Directory Service (ADS), LAN Authentication Service*)
- ix. Storage and Server infrastructure
- x. Remote connectivity and Virtual Private Network (VPN) services
- xi. Data Backup/Restoration systems

#### **10.3.4 Critical Application Services**

- ii. University Integrated System
- iii. University Website, Web services and Virtual Learning Environment (VLE)
- iv. Library Management System
- v. Pastel Accounting Services
- vi. Belina HR Services
- vii. Email Services

### 10.3.5 Applicable risk to availability;

- i. Inadequate capacity management (hardware, software, staff, service providers)
- ii. Physical Damage to ICT Infrastructure (theft, fire, floods)
- iii. ICT system failures
- iv. Inadequate IT continuity and disaster recovery planning
- v. Disruptive and destructive cyber-attacks

### 10.4 Prioritization of recovery

<b>Priority 1</b>	
<b>System</b>	<b>Estimated Time to Recover</b>
Internet Service	24 hours using DR site 40 days for new equipment installation
LAN Connectivity	24 hours using DR site 40 days for new equipment installation
Authentication and authorization systems (ADS, LAN Authentication Service)	24 hours using DR site 40 days for new equipment installation
Storage and Server infrastructure	24 hours using DR site 40 days for new equipment installation
Remote connectivity and VPN services	24 hours using DR site 40 days for new equipment installation
Data Backup/Restoration systems	24 hours using DR site 40 days for new equipment installation

<b>Priority 2</b>	
<b>System</b>	<b>Estimated Time to Recover</b>
University Integrated System (UIS)	24 hours using DR site 40 days for new equipment installation
University Web server, Web services and VLE	24 hours using DR site 40 days for new equipment installation
Library Management System (OPAC)	24 hours using DR site 40 days for new equipment installation
Pastel Accounting Services	24 hours using DR site 40 days for new equipment installation
Belina HR Services	24 hours using DR site 40 days for new equipment installation
GSuite Email Services	Service is hosted in the cloud and will not be affected by a campus incident. Access

	is dependent on availability of Priority 1 authentication and authorization systems.
--	--

10.4.1 For purposes of this Policy, “Estimated Time to Recover” is the duration of time and a service level within which a business process must be restored after a disaster or disruption in order to avoid unacceptable consequences associated with a break in business continuity.

## **10.5 Disaster Recovery Plans**

10.5.1 Each Key Business System must have a Disaster Recovery Plan documented for when hardware, software or Networks become critically dysfunctional or cease to function (short term to long term outages).

10.5.2 This Plan should include an explanation of the magnitude of information or System unavailability in the event of an outage and the process that would be implemented to continue operations during the outage.

10.5.3 In addition, the feasibility of utilising alternative off-site computer operations should be addressed.

10.5.4 The Disaster Recovery Plan must include:

- i. An Emergency Mode Operations Plan for continuing operations in the event of temporary hardware, software or Network outage. This Plan should contain information relating to the end user process for continuing operations.
- ii. Off-Site Backup and Recovery Site Plan for returning functions and services to normal on-site operations when a disaster is over.
- iii. A procedure for periodic testing, review and revision of the Disaster Recovery Plan for all affected Systems, as a group and individually as needed.

## **10.6 Data Backup Plans**

10.6.1 A backup plan enables the ICT Department to keep backup information in a readily accessible format so that any person authorized can easily read or restore information when and if required. This will ensure that university data is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster

10.6.2 To ensure that no loss of data occurs, a strict backup routine is required. It is also important that the job of doing the backups is given to one person.

10.6.3 Each system owner and ICT officer in charge will develop and implement a Data Backup Plan or SOP for data backup.

10.6.4 To ensure that no loss of data occurs, a strict backup routine is required. It is also important that the job of doing the backups is given to one person. Such Plan should define the following:

- i. Who is responsible for taking reasonable steps to ensure the backup of university data, particularly sensitive data and confidential data;
- ii. A backup schedule;
- iii. The Key Business Systems that are to be backed up;
- iv. Where backup media is to be stored and workforce members who may access the stored backup media;
- v. Where backup media is to be kept secure before it is moved to storage, if applicable;
- vi. Who may remove the backup media and transfer it to storage;
- vii. Restoration procedures to restore Key Business System Data from backup media to the appropriate System;
- viii. Test restoration procedures and frequency of testing to confirm the effectiveness of the Plan;
- ix. The retention period for backup media; and
- x. A method for restoring encrypted backup media, including encryption key management.

#### 10.6.5 Backup Measures

- i. Server configuration files must be backed up so as to enable a quick recovery from disasters.
- ii. The configuration files for network equipment must be backed up.
- iii. Databases and Applications - Database files must be backed up.
- iv. Installation CDs and DVDs must be backed up as soon as they are received.
- v. Before any change can be effected on the servers, network equipment and database, a backup shall be made.
- vi. All backups shall be logged in the backup log book and be tested for future restoration before being recorded as a backup.
- vii. The backing up database should be carried out at night or early in the morning where there will be no users accessing the system and other programs affecting the bandwidth of the network.
- viii. From time to time check to see if the backed up databases are in correct format and that they can be restored.
- ix. Backup shall be made on secondary storages, backup server, and offsite
- x. Backups can also be done on other servers and or different desktop hard drive machines or external hard drives.
- xi. Offsite backups shall be established.

- xii. A SOP should be provided for the establishment of an Offsite backup. The procedures for access and use of the site should be articulated also.

## **10.7 Systems log review**

10.7.1 A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network.

10.7.2 The ICT Department together with the user department for each system shall:

- i. Carry out all log views every 6 months.
- ii. Produce log reports after every system log review.
- iii. Regularly analyse account information logs such as the number of user login attempts per given time.
- iv. Monitor password change activities, general login activities, data modification logs, bandwidth consumption logs, risk application logs.
- v. Ensure that log review shows who did what at what time, what happened.
- vi. Ensure that users should not be able to monitor reviews in their own accounts.

## **10.8 Contacts and Resources**

10.8.1 For questions regarding overall university ICT operations and policies, contact the university ICT Director.

10.8.2 For questions regarding the ICT Services, Self Service Portal, university website and VLE, contact the Operations Manager.

---

## **11. ICT ASSET MANAGEMENT POLICY**

---

### **11.1 Introduction**

- 11.1.1 Management of ICT assets is crucial to ensure maximum return on investment (ROI) of ICT infrastructure and confidentiality of data contained.
- 11.1.2 The ICT Department has the overall responsibility of managing the procurement, registration, allocation, replacement and disposal of ICT assets.

### **11.2 Policy Objectives**

- 11.2.1 To guide the overall management of all university ICT assets and services towards ensuring standardization of all ICT related assets, transparency, timely delivery, quality assurance, value for money as well as compatibility with existing infrastructure and services.

### **11.3 ICT Asset Procurement and Registration**

- 11.3.1 ICT Assets include, but not limited to; computers, servers and tablets, software, printers, projectors, audio-visual products and services, ICT infrastructure, and IT contractors and consultants
- 11.3.2 Procurement of ICT assets shall be subject to budgetary allocations and availability of funds.
- 11.3.3 An ICT asset purchased with the Chinhoyi University of Technology ICT budget belongs to Chinhoyi University of Technology.
- 11.3.4 An ICT asset acquired through different projects (with their own budgets) or donations belongs to Chinhoyi University of Technology.
- 11.3.5 Such ICT assets mentioned in item 11.3.1 and 11.3.3 must be registered/recorded in the ICT Asset Register and University Main Asset Inventory.
- 11.3.6 The ICT Department shall ensure that all ICT assets supplied meet the prescribed requirements before accepting delivery.
- 11.3.7 The ICT Department shall ensure that all ICT assets are processed and tagged before they are issued to end users.
- 11.3.8 The ICT Department shall administer the control and security of asset held in stock for issuing and awaiting re-issue or disposal;
- 11.3.9 The ICT Department shall update and maintain the accuracy of the ICT asset register system as soon as a change is made.
- 11.3.10 The ICT Department shall check if the asset is returned with the same system and network configuration as initially issued with, where this is applicable.



- 11.3.11 The User Departments shall formally request for ICT assets through the ICT main Helpdesk.
- 11.3.12 An end user issued with an ICT asset shall take good care and responsibility for the asset issued to them until it has been returned to the ICT Department for redeployment or disposal.
- 11.3.13 An end user issued with an ICT asset shall ensure that the ICT asset is not moved to another location or transferred to another person without the consent of the ICT Department.
- 11.3.14 An end user issued with an ICT asset shall report the loss or theft of an ICT asset immediately to the Head of ICT Department via the ICT main Help Desk and will also report the theft to Campus Protection Services.
- 11.3.15 An end user issued with an ICT asset that is not performing well shall report any defects and return the asset immediately to the ICT Department via the ICT Help Desk.
- 11.3.16 The ICT Department shall facilitate asset return to the supplier subject to the asset meeting warranty conditions as specified in the supplier warranty conditions on the quotations which were used when the asset was procured and also as recorded in the asset register.
- 11.3.17 An end user issued with an ICT asset shall return all ICT assets to the ICT Department upon replacement, when it is no longer required for university business i.e. obsolete or when the holder leaves the university unless the conditions of service of the employee states that the ICT asset may be surrendered to the employee upon retirement/resignation/end of contract.

#### **11.4 ICT Asset Classification and Allocation**

- 11.4.1 The ICT Department has the responsibility of allocating all ICT assets.
- 11.4.2 The ICT Department shall ensure that the asset is signed for by the end user department/user when collected from or returned to the ICT Department and is recorded in the ICT asset register system.
- 11.4.3 The ICT Department shall give correct and appropriate advice to users on the correct handling of ICT assets.
- 11.4.4 Allocation of ICT assets shall be based on department/school demand, but should fall under allocation classification as shown below.
- 11.4.5 In case of funds constraints, employees shall be accommodated with other than entitlement.

11.4.6 Employees (Engineers/Technical/Programmers/Analysts/Researchers) who have legitimate need for higher computing power (using cutting edge technology to better fulfil their job responsibilities) may get allocation above their designation after clearly justifying the demand. The end of life of such allocation will correspond with the designation level of the allocation.

## 11.5 Allocation Classification

Designation Grade	Computer	PDA	Lifespan	End of Life
<b>Grade 1-3</b>	As per Contract	As per Contract	Computer - 3 PDA - 2	As per Contract
<b>Grade 4</b>	Laptop/ Notebook Desktop New	Tablet/Phone	Computer - 3 PDA - 2	Laptop – Personal Desktop- Return to ICT PDA – Personal
<b>Grade 5</b>	Laptop Business Class / Desktop New	Tablet/Phone	Computer - 3 PDA - 2	Laptop – Option to Purchase at depreciation value or Return to ICT Desktop- Return to ICT PDA – Personal
<b>Grade 6 -7</b>	Laptop Business Class / Desktop New	Tablet/Phone	Computer - 3 PDA - 2	Laptop – Option to Purchase at depreciation value or Return to ICT Desktop- Return to ICT PDA – Personal
<b>Grade 8 – 9</b>	Desktop New	-	Computer - 3	Desktop- Return to ICT
<b>Grade 10-13</b>	Desktop Out of Old stock	-	Computer - 3	Desktop- Return to ICT

## 11.6 Replacement of ICT Asset

11.6.1 As an ICT asset ages, it becomes more vulnerable to failure and the support cost rises. In order to maintain the productivity of the end user, the asset needs to be upgraded or replaced on a periodic basis.

11.6.2 Assuming that sufficient budget exists, computers should be replaced on a regular recurring basis which is based on Asset Average Life as guided by the ICT Equipment Replacement Policy /indicated in the table below;

### 11.6.3 Asset Average life (Lifespan)

Asset Description	Average lifespan
Personal Digital Assistant (PDA) (including Tablet, Phone)	2 Years
Image or graphics processing equipment (including LCD/LED display, Printer, Plotter, UPS and Scanner etc.)	5 Years
Computer (Including desktop, Notebook, laptop etc.)	3 Years
Active and Passive Networking equipment (including modem, routers, servers, switches, cabling infrastructure, IP systems, broadband connectivity equipment, security and authentication infrastructure)	10 Years

- 11.6.4 No computer will be replaced before the completion of the prescribed life span or proper justification duly endorsed through the concerned head of department.
- 11.6.5 Replacement of stolen ICT assets is upon provision of a completed ICT goods removal signed by the ICT Department Manager, a police report and clear justification from the user and the requesting departmental head, and availability of funds.
- 11.6.6 Replacement of mutilated, defacement, malfunction ICT asset is upon clear justification from the user and the requesting departmental head, and availability of funds.
- 11.6.7 Respective Committees or the ICT Director may approve premature condemnation up to 1 year earlier than the end of average life.
- 11.6.8 Users in custody of ICT assets must neither attempt to open any asset nor to send the asset for external repair as this is the responsibility of the ICT department. The attempt to do the prohibited action might also invalidate the device warranty.
- 11.6.9 The ICT Helpdesk can be contacted to determine if the asset falls under warranty and ensure warranties on assets are not voided when upgrades or transfers are done.

### 11.7 ICT Asset Monitoring

- 11.7.1 Coordinating ICT asset audit activity such as annual inventory checks for management reporting.
- 11.7.2 The ICT Asset issued to any individual against his post remains in his custody and can be used for any departmental/sectional CUT business. Though the asset is under individual's custody, it remains in actual allocation to the respective section/department.

11.7.3 No user is allowed to carry or shift any asset from one place to another without proper handing/ taking over and written approval from the ICT Department.

11.7.4 The ICT Department shall monitor/audit all user allocated devices to ensure:

- ii. All devices are accounted for;
- iii. The current owner / location is known;
- iv. Owners of devices with privileged access are known;
- v. Devices allocated to individuals are known;
- vi. Devices have appropriate security updates

## **11.8 ICT Asset Disposal**

11.8.1 Disposal of retired ICT assets shall comply with the Chinhoyi University of Technology Disposal Procedures.

11.8.2 Software disposal will rely on the system support cycle of the software developer company.

11.8.3 Ensuring that any ICT asset that is retired is disposed of according to the ICT Asset Disposal Procedure.

---

## **12. ELECTRONIC COMMUNICATIONS POLICY**

---

### **12.1 Introduction**

- 12.1.1 Electronic communications systems that utilize the university Information and Communication Technology are not an open forum, but rather are owned and operated by the university to promote research, teaching, learning, innovation and industrialization and to conduct official university business.
- 12.1.2 Authorized users may use these systems only within the scope of university Information and Communication Technology Policies and Procedures. Electronic communication systems include, but are not limited to: all electronic mail and Instant Messaging systems, electronic bulletin boards, web content, and Internet access.

### **12.2 Policy Objectives**

- 12.2.1 To guide the overall management of university electronic communications infrastructure and services.

### **12.3 Internet and E-mail**

- 12.3.1 The university will normally provide an email account to all staff and students, based on their duties or activities at the university.
- 12.3.2 The ICT Director may also authorise the provision of an email account for alumni, students on attachment at Chinhoyi University of Technology, and visiting lecturers, as well as other guest users. Departments/units have the prerogative to request for these services on behalf of the above.
- 12.3.3 All email accounts and associated addresses are the property of the university.
- 12.3.4 The centrally administered e-mail account will be considered the individual's official university e-mail address.
- 12.3.5 It is the responsibility of the account holder to ensure that email received at his/her official university address is attended to in a timely manner.

### **12.4 Creation and deactivation of accounts**

- 12.4.1 Staff accounts are created when the Human Resources department has notified the ICT Department of new employees that have joined the university.
- 12.4.2 Each User will have an email account created, from the university domain (abc@cut.ac.zw) or from university sub-domain e.g. (abc@hotel.cut.ac.zw) which will be centrally administered.
- 12.4.3 CUT email service is terminated when the Human Resources department has notified the ICT Department that the employee is no longer an employee of CUT.

## **12.5 Prohibited Use**

- 12.5.1 The university email system must not be used for the creation or distribution of any disruptive or offensive messages, including but not limited to: offensive comments about race, gender, disability, age, sexual orientation, religious belief and practice, political belief, or national origin.
- 12.5.2 Individuals who receive any electronic communications with objectionable content should report the matter to the ICT department.
- 12.5.3 Use of private emails for university business is strictly not allowed.
- 12.5.4 Subscribing to sites whose business is not using CUT corporate email is strictly not allowed.

## **12.6 Mass Emailing**

- 12.6.1 Mass Emailing over the university Information and Communication Technology Network from the university must be approved by the Office of the ICT Director.
- 12.6.2 Examples of Mass Emailing include, but are not limited to, sending the email to “allstaff” user group or any group of employees or students.

## **12.7 Signatures**

- 12.7.1 Signatures in Emails and other electronic messages may contain some or all of the following only: name, title, department name, name of university, and workplace contact information (phone number, fax number, mailing address, Email address). Quotations, such as proverbs etc. are not allowed in signatures.

## **12.8 Monitoring**

- 12.8.1 The university may monitor communication on the university Information and Communication Technology without prior notice, but is not obliged to

---

## 13. SOCIAL MEDIA POLICY

---

### 13.1 Introduction

- 13.1.1 Social media is a powerful tool to connect with the wider world, for students it offers opportunities to grow their depth of learning and engage in unique opportunities, as well as grow employability opportunities. For staff it offers a unique opportunity to engage with various social and professional networks and to some extent to engage with students.
- 13.1.2 This university policy is designed to aid students and staff in using social media effectively, safely, and responsibly; whilst avoiding compromising their own personal safety, or the university's security, and reputation.

### 13.2 Policy Objectives

- 13.2.1 To encourage the responsible use of social media by Chinhoyi University of Technology staff and students
- 13.2.2 To outline the responsibilities for individuals using social media for Chinhoyi University of Technology purposes
- 13.2.3 To highlight the potential risks of using social media for personal use
- 13.2.4 To provide clear guidelines on how breaches of this policy will be addressed to protect the reputation of Chinhoyi University of Technology, its students, and staff and partner organisations.

### 13.3 Social Media Definition

- 13.3.1 Social media describes online communities and networks that provide a base for interactions and the exchange of user-generated content. They allow people to share information, opinions, knowledge and interests.
- 13.3.2 Examples of popular social media sites include but are not limited to; WhatsApp, Instagram, LinkedIn, Twitter, Facebook, YouTube, Pinterest, Vimeo, Blogs, and other online chat forums.

### 13.4 Best Practices

- 13.4.1 Social Media users should adhere to the following points of best practice;
- 13.4.2 Users must note that third parties including the media, employers and law enforcement agents can access profiles and view personal information such as pictures, videos, comments and posters. Inappropriate material found by third parties affects the perception of you and the university and can have a negative impact on your future prospects.

- 13.4.3 Users must ensure privacy of their social media platforms through reviewing their security settings regularly.
- 13.4.4 Users must respect personal privacy and that of others.
- 13.4.5 Users must be familiar with specific professional practice and confidentiality rules for their study area or work area.
- 13.4.6 Users must observe copyright and intellectual property right laws, thus before publishing anything ensure that you have sought the permission of the owner.
- 13.4.7 Users must not use the university logo or associated logos or any corporate identity material on any social media unless expressly permitted to do so.
- 13.4.8 The university logo can only be used on official university social media and other online channels that are identified as official Chinhoyi University of Technology accounts and maintained by the social media team within the Directorate of Marketing and Public Relations.
- 13.4.9 Users should be aware that they are representing the Chinhoyi University of Technology when posting comments, liking, sharing or responding to comments made by others on social media.



---

## **14. E-LEARNING POLICY**

---

### **14.1 Introduction**

- 14.1.1 This policy is made up of issues related to e-learning, e-safety and best practices to ensure that e-learning platforms are used properly and according to the university's ICT policy.

### **14.2 Policy Objectives**

- 14.2.1 To maintain and service the current available e-learning technologies.
- 14.2.2 To train and educate the students and staff on how to make use of the available e-learning resources.
- 14.2.3 Ensure that e-learning will be incorporated into quality assurance assessment.

### **14.3 Virtual Learning Infrastructure**

- 14.3.1 The ICT Department shall ensure that video learning technologies are in place for online lectures.
- 14.3.2 Interactions within Chinhoyi University of Technology virtual learning environments shall be guided by the same rules as those of physical classrooms.
- 14.3.3 The ICT Department shall design and maintain an enterprise Virtual Learning Environment (VLE).
- 14.3.4 The ICT Department shall develop and maintain the university staff and student e-portal to facilitate the uploading of learning materials, tests, assignments by academic colleagues for students.
- 14.3.5 In collaboration with the School of Academy, the ICT Department will hold e-learning training and workshops for academics and students.
- 14.3.6 The ICT Department shall avail resources for activities that seek to further the knowledge and understanding of e-learning technologies.

### **14.4 Intellectual Property Rights**

- 14.4.1 Chinhoyi University of Technology has total control and ownership of the substantive and intellectual content of their online course materials that they have with respect to those offered in a traditional classroom format, at the time of production, at any time during their use, and thereafter.
- 14.4.2 No one may access or use a member's online course and content without written permission from that instructor.
- 14.4.3 In the event that the instructor of record is unable to provide permission, then access may be granted by the appropriate administrator.

## **14.5 Confidentiality and Privacy**

- 14.5.1 Student and staff records and work shall be subject to the same protection and expectations of confidentiality and privacy that are in effect for traditional modes of instructions.

Two handwritten signatures in black ink, one on the left and one on the right, both appearing to be in cursive script.

---

## **15. STATEMENT OF ENFORCEMENT**

---

- 15.1.1 Interpretation of this ICT policy rests within the ICT Department.
- 15.1.2 The ICT Department has direct responsibility for maintaining and guiding implementation of all policies contained in this policy document.
- 15.1.3 Violations of any of the policy areas listed here within shall be addressed by the appropriate university mechanism as guided by the Innovation, Commercialization & Industrialization Committee.
- 15.1.4 ICT Department will ensure the policies' enforcement and university wide dissemination as well as awareness sensitization of this policy.
- 15.1.5 ICT Department shall in partnership with the Innovation, Commercialization & Industrialization Committee be responsible for monitoring the implementation and compliance of these policies and where necessary shall take appropriate remedial measures.

## 16. APPENDIX A: DEFINITION OF TERMS USED IN THE DOCUMENT

Authorized User(s): Person(s) authorized by the university to use the university Information and Communication Technology including but not limited to staff, Students, and guests, within the limits of such person's authorization.

Backup: The process of periodically copying all of the files on a computer's disks onto a magnetic tape or other removable medium.

Certificate: A set of Security-relevant data issued by a trusted third-party organization, together with Security information which is used to provide the integrity and data origin authentication Services for the data (Security Certificate).

Chain Email: A term used to describe Emails that encourage you to forward them on to someone else.

Change Management: The process of requesting, developing, approving, and implementing a planned or unplanned change within the ICT infrastructure.

Consent: Refers to any manifestation of specific unequivocal, freely given, misinformed expression of will by which the data subject or his or her legal, judicial or legally appointed representative accepts that his or her data be processed.

Computer: Means any portable and non-portable electronic programmable device used or designed, whether by itself or as part of a computer network, a database, a critical database, an electronic communications network or critical information infrastructure or any other device or equipment or any part thereof, to perform predetermined arithmetic, logical, routing or storage operations in accordance with set instructions.

Computer system: Means interconnected or related computer devices, one or more of which uses a programme to perform the automatic processing of data, exchange data with each other or any other computer system or connect to an electronic communications network;

Computer Resources: Means all computer hardware, software, communications devices, facilities, equipment, networks, passwords, licensing and attendant policies, manuals and guides.

Pornography: Includes any representation, through publication, exhibition, cinematography, electronic means or any other means whatsoever, of a person engaged in real or simulated explicit sexual activity, or any representation of the sexual parts of a person for primarily sexual purposes;

Data: Means any representation of facts, concepts, information, whether in text, audio, video, images, machine-readable code or instructions, in a form suitable for communications,

interpretation or processing in a computer device, computer system, database, electronic communications network or related devices and includes a computer programme and traffic data;

Demilitarized Zone (DMZ): Any un-trusted Network connected to, but separated from, the university's Information Technology Network by a Firewall, used for external (Internet/partner, etc.) access from within the university, or to provide information to external parties.

Denial of Service (DoS): An attack on a computer system or Network that causes a loss of Service to users, typically the loss of Network connectivity and Services by overloading the computational resources of the victim system.

Domain Name System (DNS): A system that stores information about computer and Network names in a kind of distributed Database on Networks, such as the Internet.

Email Bomb: Causing a user's Email account to reach maximum storage capacity by the excessive sending of Email messages for the sole purpose of being malicious.

Encryption: The process of making data unreadable to unauthorized entities by applying a cryptographic Algorithm (an Encryption Algorithm).

Host: Any computing device attached to a computer network.

ICT Infrastructure: The network, computers, servers, storage, database and solutions technologies managed by the ICT department

ICT: Information Communication Technology.

Internet Protocol (IP) Address: A unique number used by machines (usually computers) to refer to each other when sending information through the Internet.

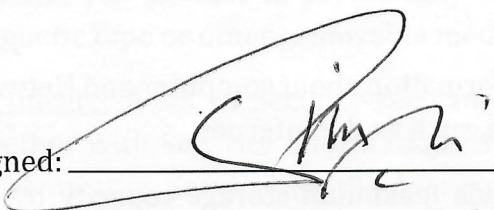
IP Security (IPsec) Concentrator: A device where IPsec connections merge into a Network and are no longer encrypted.

IP Security (IPsec): A standard for securing Internet communications by encrypting and authenticating all data.

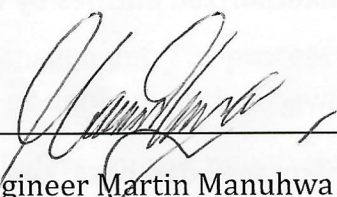
MAC Address: A code on most forms of networking equipment that allows for that device to be uniquely identified.

Unauthorized Disclosure: The intentional or unintentional revealing of restricted information to people, both inside and outside the university, who are not authorized to know that information.

Unauthorized Users: Use of the University Network by person(s) who are not Authorized Users, or use of the University Information and Communication Technology Network in violation of the law or in violation of the University Information and Communication Technology Policies and Procedures.

Signed:   
Professor David Jambgwa Simbi - Vice Chancellor

Date: 29<sup>th</sup> March 2023

Signed:   
Engineer Martin Manuhwa - Council Chairperson

Date: 05 April 2023