Information Technology Policy, 2023

Policy Documents Digitalization of TU

June, 2023

TABLE OF CONTENTS

1. INTRODUCTION

1.1. CONTEXT

Tribhuvan University's Information Technology (IT) policy establishes university-wide comprehensive strategies to safeguard the confidentiality, integrity, and availability of its information assets. This policy aims to guide the ethical development, maintenance, and security of various IT resources and services, including computers, networks, servers, software, and online platforms like e-learning, emails, and web hosting.

The university will improve, maintain, and oversee IT resources in order to boost its services and improve global-centric teaching and learning experiences. TU will assume the authority to monitor resource utilisation and resolve user interactions. This policy approach guarantees that IT infrastructure and services are well-matched to changing higher education and service needs, while also encouraging responsible use and practices.

1.2. BACKGROUND

Tribhuvan University (TU), established in 1959, is the first institution of higher education in Nepal. Tribhuvan University is a public university that runs five institutes: Agriculture & Animal Science, Engineering, Forestry, and Medicine and Science & Technology. Similarly, its four faculties: Education, Humanities & Social Science, Law and Management and four research centers (CEDA, CNAS, RECAST and CERID) have been providing the academic excellence in the country. The university has produced the largest number of graduate and post graduates in Nepal.

TU intends to adopt cutting-edge technology to provide students and other stakeholders with the access to its services as demanded by the time and technical evolution. This information technological policy aims to create an effective, professional, legal, ethical, and equitable environment to have an access to IT facilities across TU in order to improve educational quality.

TU-IT unit under the IT and Innovation Center will assume the authority to enforce these policies across all IT resources of TU.

1.3. SCOPE OF THESE POLICIES

This policy applies to the University's wings and its affiliated campuses. They also apply to individuals such as authorities, teachers, personnel, and others who utilise TU IT resources both on and off campus. Similar regulations apply to the use of TU information on both official and non-TU devices. It should be noted that any national legal or regulatory requirements that are stricter than these policies will supersede these policies.

1.4. REVIEW OF THESE POLICIES

These policies and standards will be reviewed periodically and a new version of the document will be issued. Revised versions will also be issued if there are any significant changes in technologies or the environment.

2. COMPLIANCE TO THESE POLICIES

2.1. COMPLIANCE AND MONITORING OF THESE POLICIES

TU-IT unit will have the authority to enforce these policies through appropriate technology, and to audit and check compliance (manually or through technology) of all TU's IT resources. Compliance to policies will also be monitored in the usual way to determine whether IT controls protect corporate assets, ensure data integrity and are aligned with the educational overall goals through IT audits.

2.2. ACTION AGAINST THE BREACH OF THESE POLICIES

Actions that will be taken in such situations will be as follows:

- Violating this policy means an unethical practice, which could even mean dismissal as per university rules and regulations for serious misconduct. If a violation invites serious consequences, legal authorities will be informed.
- Staff using TU's IT systems and resources for harmful content may face strict disciplinary actions, regardless of legal outcomes.
- Access to Wi-Fi, Internet, email, e-learning and more can be withdrawn during investigations into suspected misuse.
- Users could be personally held accountable and face legal consequences if they break the country's laws. Claiming no intent won't excuse harassment allegations.

3. VISION STATEMENT

TU will gradually adopt IT-based appropriate services for knowledge management and service delivery to improve quality education.

4. MISSION STATEMENT

TU will enhance its educational excellence by gradually integrating appropriate IT-based tools and services to knowledge development process and academic service delivery with an expectation that it will result in a better and more impactful teaching and learning environment.

5. GOALS/OBJECTIVES:

5.1 Broadband Connectivity Enhancement: Ensure high-speed, reliable internet connectivity throughout the university's campus, allowing for smooth communication and access to online academic services and resources.

5.2 Optimal Digital Infrastructure Utilization: Maximise the use of digital technologies and resources to improve administrative efficiency, academic operations, and research endeavours.

5.3 Effective Learning Management System (LMS) Operation: Manage and maintain the university's Learning Management System (LMS) effectively, offering a user-friendly platform for course delivery, resource sharing, and student engagement.

5.4 Creation of Interactive Learning Resources: Create and disseminate digital learning materials that encourage learners to engage in interactive and collaborative learning experiences.

5.5 Strategic Use of Educational Management Information System (EMIS) and Automation: Implement EMIS and automation solutions to improve the efficiency of academic processes, student management, reporting and administrative tasks.

5.6 Empowerment of Human Resources: Provide comprehensive training and support to equip professors and staff with digital skills, encouraging effective technology integration and digital pedagogy for improved teaching and learning results.

6. KEY DIGITATION IT POLICY STATEMENTS

6.1. BROADBAND CONNECTIVITY AND INTERNET ACCESS

6.1.1. NETWORK SYSTEM ACCESS

a) TU ensures comprehensive and reliable broadband connectivity throughout the university campus, including academic buildings, administrative building, and common areas, such as the library, to promote seamless access to online resources.

b) Computing Devices connected to the university network should have an IP address assigned by the IT Center at university campus and central offices of TU.

c) Access to the TU information network is permitted only with devices authorized and set up by IT Center and IT support unit of TU's institutions.

d) Any access to the network bypassing the official gateways, firewall etc. is forbidden.

e) Users should not disclose their access details to outsiders nor allow outsiders to access TU resources in any way except in the case permission granted from IT Center or IT support unit.

f) Users should not download, install or run any unauthorized programs and illegal or unethical computing activities on their computing devices.

6.1.2. INTERNET ACCESS

a) TU promotes equitable access to broadband connectivity for all members of the university community, regardless of location or department, fostering inclusivity and equal opportunities for learning and collaboration.

b) All Internet access will be granted through the configuration set up by the IT team. All internet access will be scanned for viruses and monitored and recorded and filtered to check an inappropriate access.

c) Internet access will be password-protected and exclusively available for students, staff, faculty, and alumni of the university.

d) The Internet is not to be used to access or disseminate illegal, objectionable, or obscene materials or to engage in any conduct, which may be considered to be provocative, abusive, or harassing. The internet is not to be used to conduct personal business for profit. Chat rooms and adult-oriented sites are specifically prohibited at central level and campus level.

e) All users must ensure that they do not knowingly or unknowingly enter into any agreement with third parties on behalf of TU without explicit approval from appropriate authority.

f) TU will not provide a home internet connection except for IT personnel who have been allowed to work from home for some special reasons. Any internet connection at home will require authorization from authorities.

g) All internet access will be provided to the users through the TU firewall set up as per the policy and standard.

6.2. DIGITAL INFRASTRUCTURE DEVELOPMENT POLICY

a) TU ensure the efficient and secure operation of the university's data center at IT and Innovation center, including secure hardware, data backup, disaster recovery planning, and adherence to industry best practices for data center management.

b) All IT units will be equipped with computers, servers, data storage, firewalls, power backup and different software to manage these devises resources.

c) Standards for the development and expansion of Local Area Networks (LAN) and Wide Area Networks (WAN), focusing on scalability, security, and seamless integration to facilitate efficient communication and resource sharing will be defined.

d) The university will also use government support data centers to backup different information for recovery purpose.

e) The university plans to build an internal network for sharing private information within units, campuses, and departments, primarily for managing internal activities like accounting, examination, and administration.

f) The university plans to develop an extranet for secure, controlled access to information and operations for stakeholders.

g) IT infrastructures must be secured with passwords, biometrics, and multifactor authentication. Data will be stored on secure servers with appropriate access control rights, and access restricted to authorized individuals.

h) University will deploy surveillance cameras and CCTV for crime deterrence and illegal activities, enhancing security and monitoring.

i) Video conferencing systems and virtual learning tools for online collaboration and teaching activities will be enhanced.

6.3. LEARNING MANAGEMENT SYSTEM POLICY

a) TU will promote the use of open-source Learning Management Systems (LMS) for educational purposes, encouraging cost-effective solutions that offer customization and flexibility while adhering to security and compatibility standards.

b) LMS will implement a centralized approach to LMS hosting, ensuring a consistent user experience, efficient resource allocation, and streamlined administration, while also enabling scalability to accommodate growing user demands.

c) IT Unit and ODEC will facilitate access to the LMS for all campus units, departments, and teaching staff, promoting inclusivity and fostering a collaborative environment for sharing educational content and resources.

d) TU IT unit will regulate the usage and access to the Microsoft Teams-based video conferencing system for LMS, ensuring proper integration, privacy controls, and user training to facilitate effective online communication and collaboration.

e) TU will provide a platform for managing and delivering online courses and resources to students and faculties.

f) Access to the LMS will be restricted to authorized personnel only. Access will be granted based on a need-to-know basis, and access control measures, such as strong passwords and two-factor authentication will be implemented to ensure security.

g) Each student and faculty member will be assigned a unique user account, which will be used to access the LMS. User accounts will be maintained and managed by the IT unit, ODEC and IT unit of campus.

h) The LMS will be designed and operated in compliance with all relevant data privacy regulations. Data privacy policies will be clearly communicated to users, and measures will be implemented to ensure the confidentiality and security of user data.

i) Technical support for the LMS will be provided by the IT Units. Users will be provided with clear instructions on how to access technical support, and response times and resolution times will be defined and communicated.

j) Training and support will be provided to faculty and staff on how to use the LMS effectively. Resources, such as user manuals, video tutorials, and online forums will be made available to users.

k) Content on the LMS will be created, managed, and monitored by authorized faculty and staff of concerned subject committees, campuses or authorized academic units. Policies and procedures will be in place to ensure the accuracy, integrity, and appropriateness of content.

l) The LMS environment will be continuously monitored for performance, security, and other relevant metrics. Reports will be generated regularly to provide insights into performance and identify any areas for improvement.

m) The LMS system will be regularly maintained and updated to ensure optimal performance and functionality. System upgrades will be thoroughly planned and documented to minimize disruptions to operations.

n) All users of LMS must access the system through a designated account and system and should disable access or remove users for inappropriate behavior.

o) Environment for massive open online courses (MOOCs) will be provided to offer online courses to students all over the world, for free. Mass-scale training through MOOC learning platform. MOOC in different disciplines offered by different MOOC platforms, such as Coursera, edX, Khan Academy, etc. are free courses to learners around the world. Faculties and students will be encouraged to be aware about the MOOC learning platform appropriate for their field and self-certification.

6.4 DIGITAL RESOURCE DEVELOPMENT AND DISSEMINATION POLICY

a) TU will promote the creation, development, and share of diverse digital educational resources, such as eBooks, audio, video, text, animations, and simulation-based learning materials, to enhance the quality of higher education.

b) TU will establish state-of-the-art recording studios to facilitate the production of high-quality audio and video content for academic and educational purposes.

c) TU will actively promote sharing of digital educational resources under Open Educational Resources (OER) licenses, encouraging the free exchange of knowledge and collaboration among educators and learners.

d) TU will develop, maintain, and regularly update its comprehensive digital library, providing access to a wide range of resources, including eBooks, research papers, multimedia content, students' Theses and other relevant academic materials.

e) TU will support the creation and integration of simulation-based learning materials that offer students immersive and experiential learning opportunities, enhancing practical skills and knowledge acquisition.

f) TU will acquire subscriptions to reputable global publishers' databases, ensuring access to a wide array of scholarly resources, academic journals, and research publications for the benefit of the academic community.

g) TU will ensure that all digital resources developed and shared have accessibility features, adhering to universal design principles to make them accessible to individuals with (dis)abilities.

h) TU will implement a systematic quality assurance and review process, involving subject experts and educational technologists, to maintain the accuracy, relevancy, and effectiveness of digital learning materials.

i) TU will establish clear guidelines and procedures regarding intellectual property ownership and copyright regulations for all digital resources while also encouraging the use of appropriate licenses.

j) TU will subscribe to plagiarism detection tools to maintain academic integrity, uphold ethical standards, and prevent plagiarism in all digital content.

k) TU will integrate the policies related to the development, publication, and sharing of digital resources to the overarching IT policy of the institution, ensuring a coherent and secure technological environment for academic purposes.

l) TU will digitize traditional print materials, ensuring online access for users, and develop local digital content, such as classroom and training videos, making them available online to enrich the learning environment.

6.5. EDUCATION MANAGEMENT INFORMATION SYSTEM

a) TU will establish an EMIS system for education leaders, decision-makers, and managers to access comprehensive, reliable, and timely data for their responsibilities.

b) TU utilizes EMIS for data collection, integration, processing, maintenance, and dissemination for decision-making, policy analysis, planning, monitoring, and management in education systems.

c) EMIS at TU will manage staff and student data, organize university information, and monitor education programs' performance. It will also manage resource distribution and allocation, planning and strategizing for smooth implementation of the education system.

d) An Integrated Educational Management System (IEMS) will be used to integrate different systems to a complete framework, enabling it to work as a single unit with unified university objectives. All of the functionalities of the university will be integrated into a centralized platform.

6.6. HUMAN RESOURCE DEVELOPMENT

a) The university will promote digital leadership proficiency for university authorities, campus chiefs, deans, directors, and heads of departments to ensure digitalization and effective online/blended education management and collaborative administration in higher education.

b) The university will enforce a comprehensive digital literacy program for staff, faculties, and students, enabling them to collectively drive the institution's digitalization mission through effective and proficient use of digital tools and technologies.

c) The university will enforce comprehensive pre-service and in-service digital pedagogy training for teachers, ensuring effective teaching, learning, and skill acquisition to enhance global competitiveness.

d) The university will implement focused training on digital subject-specific tools for teachers to enhance effective teaching, learning, and skill development to respective subjects.

e) The university will establish and execute self-paced MOOC-based training programs to enhance the skills of teachers, faculty, staff, and students, fostering comprehensive capacity building.

f) The university will implement a video conferencing policy to enable comprehensive remote training and ongoing capacity development for teachers, staff, and students across end-to-end points.

g) The university will revise the training curriculum to incorporate emerging topics including cyber security, 21st-century leadership skills, and ensure regular updates to address new issues.

h) The university will Implement an online mode of training for new recruit staff to receive comprehensive services training.

6.7. UNIVERSITY AUTOMATION

a) The university will use different hardware and software tools to convert traditional paper-based office processes into electronic processes with a goal to create a paperless office. The goal is to ensure the improved productivity and expedite performance using ICT tools.

b) The university will use different systems to capture, store, and analyze data in the university.

c) Different technologies will be used to support automation to produce and deliver services with minimal human intervention. The implementation of automation technologies, techniques and processes is likely to improve the efficiency, reliability, and/or speed of many tasks that have been carried out by humans.

d) The university will focus on improving service delivery to students, faculties, staffs, and concerned stakeholders through the use of information technology.

e) Using different ICT tools helps to improve efficiency, accountability, and transparency, and reducing bribery.

f) The university will use enterprise resource planning (ERP) software to automate and manage all the activities of the university for optimal performance.

g) The university will implement different communication and collaboration tools (such as email, video conferencing, social media, online meeting and classroom tools) to communicate, collaborate, and coordinate with different people and organizations.

6.8. SECURITY, PRIVACY, SURVEILLANCE, AND PLAGIARISM

6.8.1. VIRUS PROTECTION

a) All computer systems used in the university will have anti-virus software installed. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.

b) Individual users should make sure that respective computer systems have updated virus protection software installed and maintained.

c) The virus protection software must not be disabled, bypassed or have its settings altered.

d) All viruses that are not automatically cleaned by the virus protection software must be reported to the local IT unit.

e) Users must not intentionally write, compile, copy, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any organization's computer systems.

f) Attachments to electronic mail and externally-supplied, computer-readable files, software programs, databases, word processing documents, and spreadsheets must not be executed or opened unless they have been checked for viruses.

g) Users should consult IT before plugging in any portable devices like USB drives, SD cards, CDs, DVDs etc. They can carry viruses and can cause damage to the systems. Users will be held responsible if they do not check with IT authorities on this.

6.8.2. COPYRIGHT PROTECTION

a) TU will follow copyright laws regarding protected commercial software and intellectual property of technological products and services.

b) All the materials accessed through TU network will be subject to protection using copyrights, patents, and trademarks. If any member found violating such copyright shall be treated as per the provisions of the related act.

c) All the digital contents created in any university unit will not be made available to outsiders without informed consent to the university.

6.8.3. PLAGIARISM CHECKING

a) The university will introduce a centralized plagiarism checking software across all campuses to ensure consistency and adherence to academic integrity standards.

b) The university will define specific levels (e.g., graduate, M.Phil, PhD research) where the use of plagiarism checking software is mandatory for assignments, projects, theses, and research papers.

c) The university will promote awareness campaigns that educate students and faculty about the importance of plagiarism prevention, proper citation practices, and the role of the software in maintaining academic honesty

d) The university will integrate the plagiarism checking software to the university's learning management systems to streamline the submission and evaluation process, ensuring seamless use by all stakeholders.

e) The university will establish a system for monitoring software use and generating reports on plagiarism detection rates, enabling departments to identify trends, address issues, and take corrective actions as needed.

6.9. DATA PROTECTION, BACKUP AND RECOVERY

6.9.1. DATA PROTECTION

a) Critical or sensitive data of all TU and related campuses, departments or partners must be stored in a secured server with appropriate access control rights. All data retention or storage should be in accordance with legal requirements.

b) Access to university data will be restricted to authorized personnel only. Access will be granted based on a need-to-know basis, and access control measures, such as strong passwords and two-factor authentication will be implemented to ensure security.

c) Sensitive university data will be encrypted both in transit and at rest to protect against unauthorized access and data breaches.

d) The university's IT Center will continuously monitor the university's network and systems for security threats and vulnerabilities. Any suspicious activity will be promptly investigated and addressed.

e) Regular security assessments will be conducted to identify any potential security risks or vulnerabilities in the university's network and systems. Any identified risks or vulnerabilities will be promptly addressed.

f) Faculty and staff will be provided with training on security best practices, including the importance of strong passwords, avoiding phishing scams, and safe browsing habits. Regular reminders and educational campaigns will be conducted to ensure that faculty and staff remain vigilant against security threats.

6.9.2. BACKUP AND RECOVERY

a) All the critical data will be backed up on a regular basis as per the TU backup procedure. The IT group will enter into an agreement with users for this purpose. Any data not covered by this agreement will need to be backed by the user individually.

b) All sensitive data will be backed up on a regular basis as per the requirement. The critical data will be backed up on multiple locations and media as per necessity.

c) Recovery will be done from the backup by restoring the data to the original location, or to an alternate location where it can be used in place of the lost or damaged data.

d) Different sites, such as cold sites, hot sites and warm sites will be used as per the requirement.

6.10. SECURITY OF INFORMATION TECHNOLOGY RESOURCES

a) The university will enforce strict role-based access control for servers, computing devices, routers, switches, and firewalls, limiting access to authorized personnel based on their responsibilities.

b) The university will implement a rigorous software update process to regularly update and maintain the security of software and firmware across all digital and IT infrastructures.

c) The university will use network segmentation to isolate important components and continuous monitoring to detect and respond to any strange behaviors inside the infrastructure as soon as possible.

6.11. CENTRALIZED DATA MANAGEMENT

a) The university will establish a centralized database management system to store all the data of the university. This data will be collected from different units, campuses, and departments of the university in the central data repository.

b) Each unit of the university will also develop their own database system to store their data locally.

c) Every data source must be validated before collecting data in the central database. This data will be readily available whenever needed to the authorized users of the university.

d) Data capture, validation, and processing will be automated whenever possible and data will be recorded as accurately and completely as possible.

e) Data will be protected from an unauthorized access and will be defined and presented consistently across the university.

6.12. ONLINE AND BLENDED EXAMINATION

f) TU will establish necessary infrastructure to conduct online and blended examinations for internal and external (final) evaluations.

g) The university will also use different features of online examination system/LMS to conduct assessments and quizzes.

h) The university will develop/acquire IT system following examination policy and procedures to conduct assessments and final examinations. This system will incorporate features for disability, code of conduct, and penalties imposed in case of misconduct. The system will also support online invigilated and non-invigilated exams.

i) The duration of the online/blended exam will be decided by the university.

6.13. HARDWARE RESOURCE STANDARDS

a) Procurement, management and disposal of all hardware resources (such as, laptops, desktops, networking devices etc.) will be decided by the university units such as central office, campus, dean offices, research centers etc.

b) The different hardware resources purchased in the university will be genuine if financially viable.

c) The devices will be configured, audited and deployed by the IT unit of the concerned university unit.

d) If any device is accidently damaged, the IT unit will be notified and the device will be repaired if financially viable.

6.14. USER ACCOUNT AND E-MAIL ID CREATION AND DELETION

a) All TU faculties, staff, retried staff, long-term contractors, and long-term and full-time consultants are provided with a user account within the local domain, as well as an e-mail ID for faculties and students.

b) The local HR member or staff will create predefined template to create email ID and sent it to given email of IT center an entry for all staff, contractors and consultants in the AMIS (Attendance Management Information System). Then IT unit will create the user IDs and e-mail IDs in the domain later.

c) In the corresponding domain, the IT and Innovation Centre will create user IDs and e-mail IDs.

d) IT staff do not have the authority or responsibility to set up or delete user or email IDs. This authority/responsibility is assigned with HR unit. Other user rights like changing password, adding users to group etc. will be done by IT units in consultation with line managers and HR managers.

6.15. RESPONSIBILITY FOR ASSIGNED RESOURCES

a) TU employees will be held responsible for TU information resources assigned to them and should ensure the security of their passwords and other resources.

b) Unauthorized access of TU information resources, including other people's email and other accounts, will invite disciplinary action.

6.15. OWNERSHIP OF TU INFORMATION

a) All information contained in the TU network (including servers, desktops, laptops, mobile phones etc.) is deemed to be property of the TU.

b) The University requires proper handover of information and resources to successor, designated authority, or local HR person upon leaving.

c) Portable storage devices cannot be used to store critical or sensitive data. However, if necessary, in order to provide a required business function an exception must be approved by the TU Management. Password protection of critical data on portable storage device must be ensured, and if possible, required appropriate encryption processes must be implemented.

6.16. WEBSITE HOSTING

a) The university will ensure the unified online presence of website and develop a centralized framework for the university's main website and all academic and no-academic unit specific subdomains, ensuring a consistent user experience, branding, and navigation structure across all web properties.

b) The university will implement a collaborative content management system that allows each campus to manage its subdomain content within the established guidelines while maintaining a cohesive overall management and design.

c) All external pointing websites should be hosted at IT and Innovation center TU, Government Integrated Data Center (GIDC) and other approval third party of TU.

d) Access to the integrated website will be restricted to authorized personnel only.

e) The integrated website will be designed and operated in compliance with all relevant data privacy regulations. Data privacy policies will be clearly communicated to users, and measures will be implemented to ensure the confidentiality and security of user data.

f) Technical support for the integrated website will be provided by the IT center. Users will be provided with clear instructions on how to access technical support, and response times and resolution times will be defined and communicated.

g) The integrated website will be continuously monitored for performance, security, and other relevant metrics. Reports will be generated regularly to provide insights into performance and identify any areas for improvement. Additionally, monitoring and reporting will be done to track user behavior and to optimize the user experience.

6.17. BIOMETRIC ATTENDANCE POLICY

a) The university will develop a centralized system to collect all the attendance related information from different units of the university.

b) The university will use fingerprint scanners or face detection or retina detection to record and track attendance.

c) Biometric data collected from students, teacher and staff will be securely stored and protected, and only authorized personnel will have access to it. The data will be used solely for attendance tracking purposes and will not be shared with third parties without prior consent.

d) Teachers, students and staff will be provided with clear information about the biometric attendance system and their rights regarding the collection and usage of their data. They will be given the option to opt out of the system if they choose, but they will be required to provide alternative means of tracking attendance.

e) The university will periodically review and update the biometric attendance policy to ensure that it is compliant with any legal or ethical standards, and that it continues to serve its intended purpose effectively.

6.18. IS AUDIT AND ASSURANCE POLICY

Information System Audit and Assurance professionals will implement standards to reduce errors and ensure accurate findings. These standards include engagement planning, risk assessment, performance and supervision, materiality, irregularity, and illegal acts. It must follow the following linkage standards, such as Standard 1201 Engagement Planning, Standard 1202 Risk Assessment in Planning, Standard 1203 Performance and Supervision, Standard 1204 Materiality, Standard 1207 Irregularity and Illegal Acts etc.

6.19. OPERATION OF DATA CENTER

TU will ensure the following issues to operation of data center.

a) Access Control: Access to the data center will be restricted to authorized personnel only. Access will be granted based on a need-to-know basis, and access control measures such as biometric authentication and CCTV surveillance will be implemented to ensure security.

b) Environmental Control: The data center environment will be maintained at a stable temperature and humidity level to ensure optimal performance and longevity of equipment. Regular inspections and maintenance will be conducted to monitor and maintain the environment.

c) Power Management: The data center will be equipped with an uninterrupted power supply (UPS) and backup generators to ensure continuous operation in case of power outage. Power usage will be monitored and optimized to reduce waste and minimize costs.

d) Network Security: The data center network will be secured with firewalls, intrusion detection systems (IDS), and other security measures to prevent unauthorized access and data breaches. Regular vulnerability assessments and penetration testing will be conducted to identify and address any potential security risks.

e) Data Backup and Recovery: Regular backups of data will be taken and stored off-site to ensure that critical data can be recovered in the event of a disaster or system failure. The backup and recovery process will be regularly tested to ensure reliability.

f) Change Management: Any changes to the data center environment, such as updates to software or hardware, will thoroughly be planned and documented to ensure minimal disruption to operations and minimize the risk of errors or failures.

g) Monitoring and Reporting: The data center environment will be continuously monitored for performance, security, and other relevant metrics. Reports will be generated regularly to provide insights into performance and identify any areas for improvement.

h) Physical Security: Physical security measures, such as security cameras, alarms, and security personnel will be implemented to ensure that the data center is protected against theft or unauthorized access.

i) Disaster Recovery: A disaster recovery plan will be developed and regularly updated to ensure that the data center can quickly recover from any unexpected disasters or emergencies, such as natural disasters or cyber-attacks.

j) Compliance: The data center will be designed, implemented, and operated in compliance with all relevant laws, regulations, and industry standards, including data privacy regulations, intellectual property laws, and relevant industry certifications, such as ISO 27001.

6.21. CLOUD INFRASTRUCTURE DEVELOPMENT

a) The university will acquire cloud-based services for e-learning, laboratory work, data storage etc.

b) The university will also establish its own private cloud infrastructure and house them within its data center.

7. INSTITUTIONAL ARRANGEMENT

For effective implementation, monitoring, and control this policy, the university will have different hierarchies of ICT units as follows:

a) **ICT Steering Committee:** An ICT Steering Committee of 7 members, led by the Registrar, will form an IT governance and regulatory team to implement and monitor current IT policies. The committee will guide the Information Technology Innovation Center at TU, with details on its tenure and roles to be developed later. The member of steering committee as follows:

   1) Coordinator: Registrar of TU
   2) Member: One representative from each of 9 Dean offices

3) Member: Campus Chief/Head (Representative from Campuses and Departments)
4) Member: The Head of Finance Division
5) Member: The Head of General Administration
6) Member: Faculty Member (from IT related subject campuses and Departments)
7) Member Secretary: Director, IT and Innovation Center

b) **Information Technology Innovation Center:** The Information Technology Innovation Center will implement TU's IT policy, guiding and coordinating with the ICT Steering Committee. It will identify gaps in IT development and recommend new policies for IT-based functions.

c) **IT Unit:** Functional units, including departments, campuses, schools, and directorates, will establish IT units to support faculties, staff, and students, as end users of IT policy. Campus/Department will establish three-member committee as follows:

1) Coordinator: Assistant Campus chief/Director/HoD
2) Member: Chief of Admin Section
3) Member Secretary: Chief of IT Unit

8. PLANNING, MONITORING, AND EVALUATIONS

a. University will use technology to improve the accuracy of planning by providing university leaders with the data they need to make effective decisions. Technology solutions gather data from internal and external sources, store them in a data warehouse and provide university leaders with access via a computer network. Different collaboration tools will be used to work together to plan operations and make joint decisions.

b. Monitoring and evaluation approaches are used to measure and access the success and performance of projects. The main goal is to see if a project is going according to the plan or if it needs any adjustments. The university will focus on the following activities to monitor and evaluate the digitation process:

- Periodic monitoring and evaluation of the digitization process, different infrastructures and tools used in the digitization process.
- Monitoring and evaluation of different hardware and software systems being used to manage digital resources and online libraries, administration, management, examination etc.
- Monitoring, evaluation, and revision/update of digitization policy and practices used in the digitization process.
- Use different biometric technologies to monitor students, faculties, and staff.

9. POLICY UPDATE AND DISSIMILATION

a) The university will comprehensively review all organizational policies at least once every two years or as per necessity to ensure accuracy, relevance, and compliance with evolving laws, regulations, and best practices.

b) The university will establish a policy review committee comprising relevant stakeholders from different departments to oversee the review process and make necessary updates.