Far Western University

Information Technology Policy and Strategy

2023

Contents

Abbreviations

CERT:	Computer Emergency Response Team
CMS:	Content Management System
EIMS:	Education Information Management System
EMIS:	Education Management Information System
ERPS:	Enterprise Resource Planning System
FWU:	Far Western University
HEI:	Higher Education Institution
HRD:	Human Resource Development
ICT:	Information Communication Technology
ISP:	Internet Service Provider
IT:	Information Technology
LMS:	Learning Management System
MIS:	Management Information System
MoEST:	Ministry of Education, Science and Technology
MOOC:	Massive Open Online Course
NOC:	No Objection Certificate
OER:	Open Educational Resources
UGC:	University Grants Commission

Introduction

1.1 Background

Far Western University (FWU) was established in 2010 by the Act of the Parliament as a government funded national university to function as a prime academic institution in the country in terms of academic excellence, research-based education, community engagement and partnership. It has been delivering diverse educational programs, both in undergraduate and graduate level, through eight faculties. The university has started M. Phil. and Ph. D. research degrees since February 2021. To move forward in achieving academic excellence, it has developed several strategic documents to support the mission and vision of the university. This IT policy is one of those strategic documents that shapes the responsible IT culture within and beyond the university. In fact, clear policy guidelines are needed to improve IT services of the university in response to changing needs and priorities of the university and the wider community.

As technology continues to play an increasingly important role in personal and academic lives, it is essential to ensure and secure the responsible use of IT resources at FWU. In order to develop and strengthen the university digitalization and automation, this **'Information Technology Policy and Strategies 2023'** has been prepared. All users of university must be familiar with university's IT resources and policies. And necessary steps should be taken to ensure its proper implementation. Therefore, the IT policy is a statement of a comprehensive goal and action plan for integrating ICT into all university activities.

1.1.1 Organizational Structure

The organizational structure for IT policy will be as follows:

ICT Steering Committee: A 5–11-member central level ICT Steering Committee will be the key IT governance and regulatory team, which is responsible for developing the university's IT policy, strategy and guidelines. It will also be responsible for ensuring/approving that the HEIs' IT policies and guidelines are aligned with university's IT strategy. This committee ensures that the IT policies are developed, implemented, and enforced in a coordinated and effective manner. Moreover, a few experts can be invited in specific tasks. It should also enable the university to respond quickly to changes in the technology landscape and evolving threats to IT security and data privacy. This committee is responsible for coordination and collaboration with the Sudurpaschim Province government/local governments in relation to ICT standards.

IT Director: The IT Director is centrally located (at university headquarters) and is responsible for overseeing the university's technology policy/strategy and its implementation across faculties. This individual also serves as the ex-officio

1

secretary of the IT Committee of the University. Moreover, the person will be considered as an IT focal person of the university.

IT Staff: Each faculty and affiliate campus will have a technical support staff/team, who is/are responsible for providing technical support to end users of university's IT policies (i.e. faculty/staff and students).

1.1.2 Current Status

FWU has been taking some steps towards digitalization. Currently, it has some of the systems and practices such as: centralized email system (FWU domain); centralized website management system; account management system; exam management system; online results system. It also initiated online classes and exams during the COVID-19 pandemic. Meanwhile, it developed a policy guidelines titled "वैकल्पिक माध्यमबाट परीक्षा सञ्चालन, व्यवस्थापन तथा मूल्यांकन सम्बन्धी निर्देशिका, २०७७ संशोधन सहित २०७८". Likewise, web-conferencing and remote guest sessions are also taking place. Importantly, university MIS is in place. FWU has a good internet connectivity to support the academic and administrative activities of the university. This way, FWU has prioritized some works on policy and taken some basic steps in practice.

1.1.3 Scope

This IT policy applies to all uses of FWU IT resources, whether physically located on campus or remotely. The IT resources include all those ICT related resources and systems (personal computers, laptops, smart phones, internet connections, application software, databases, removable media, etc.) under the management or control of IT services or other units of FWU. Likewise, the IT users, such as students, staff (teaching and non-teaching), casual staff, consultants, contractors and suppliers working for or on behalf of the university, and visitors to the university, can use IT resources provided by the university.

1.2 Vision

To leverage technology in order to enhance the learning, research, and administrative capabilities of the university, while ensuring the security, privacy, and ethical use of digital resources.

1.3 Mission

The motto of this IT policy is to **'Shift from digitization to digitalization'**. The mission is to provide robust and reliable IT infrastructure and services that support the academic and administrative functions of the university, including network connectivity, email, learning management systems, research computing, and administrative systems through investment in emerging technologies and best practices.

1.4 Goal/Objectives

The purpose of this policy is to establish guidelines and best practices for the use of university IT resources, which include hardware, software, networks, and data. By following these guidelines, we can minimize the risks of data breaches, cyber-attacks, and other IT-related incidents, while protecting the privacy and confidentiality of the users.
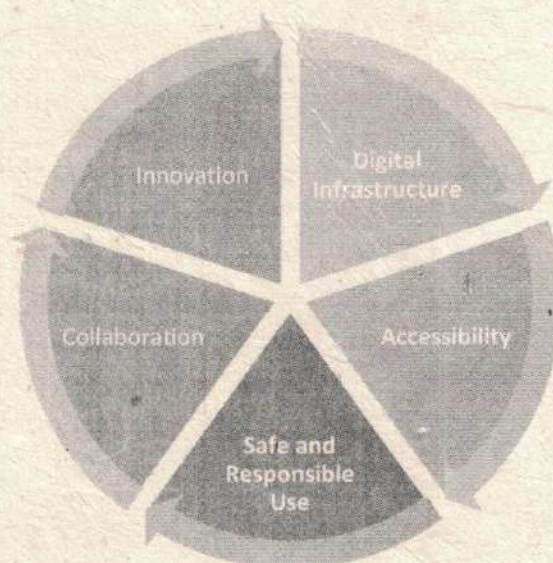
The major objectives of this IT policy are as follows:
1. To protect the security and integrity of university IT resources
2. To ensure the availability and reliability of IT services
3. To promote responsible and ethical use of IT resources
4. To support innovation and digital transformation of the university services
5. To ensure compliance with legal and regulatory requirements

1.5 Priorities

1.5.1 Digital Infrastructure

FWU focuses on developing robust digital infrastructure to support its academic and administrative activities. This includes high-speed internet, reliable computer systems, and software applications that are critical for teaching, learning, research, and administrative operations.

1.5.2 Accessibility

It is important to ensure that digital resources and tools are accessible to all members of the university community, as well as those with disabilities. This also includes making sure that websites, applications, and other digital resources are designed with accessibility in mind.

1.5.3 Safe and Responsible Use of ICT

It is important to ensure that FWU ICT resources are used in a way that promotes learning, research, and innovation while protecting the privacy and security of all members of the university community. For this, FWU prioritizes training and support programs to students, faculty, and staff to promote safe and responsible use of ICT. Likewise, FWU will use filtering and monitoring tools to block access to inappropriate content and monitor usage of ICT resources. It will also enforce consequences for misuse of ICT resources. Moreover, strong cyber security measures are necessary to protect against cyber threats, including hacking, phishing, malware, and ransomware attacks.

gaming learning materials) that support innovation, foster knowledge sharing, and enhance learning while upholding intellectual property rights and data privacy regulations.

2.6 Human Resource Development

FWU is dedicated to utilizing IT to support the continuous human resource capacity development of its employees through effective ICT training, learning management systems, and digital tools, fostering a culture of skill enhancement, professional growth, and knowledge sharing.

2.7 University and Its Campus Office Automation and EMIS

FWU is committed to implementing comprehensive university and its campus office automation solutions, including robust Education Management Information Systems (EMIS), to streamline administrative processes, enhance operational efficiency, and improve data-driven decision-making across all campuses, departments and other units. University e-governance will eventually be ensured (i.e., using an ERP system integrating finance and administration).

2.8 University Intellectual Property Security, Privacy, Plagiarism System, Surveillance and Copyright Law

To protect the rights and interests of individuals and the institution, FWU is committed to ensuring the security and privacy of intellectual property, putting in place efficient systems for detecting plagiarism, upholding copyright laws, and conducting surveillance operations within legal and ethical boundaries.

2.9 University Data Protection, Back up and Disaster Recovery

To secure crucial data and lessen the effects of potential disruptions or data loss occurrences, FWU will establish strong data security mechanisms, regular backups, and comprehensive disaster recovery plans.

2.10 IT System Security, Safety, Avoidance and Prevention from Attack

FWU will maintain to secure IT environment by implementing comprehensive security measures, ensuring the safety of information assets, and proactively preventing and mitigating potential cyber-attacks, vulnerabilities, and threats.

2.11 Centralize HEIs Data Management

To ensure effective and safe data storage, retrieval, and utilization, FWU will centralize university data management by establishing standardized procedures and putting in place strong systems.

2.12 Online/Open/Blended Examination

FWU will gradually introduce safe, reliable, and inclusive online, open, and blended examination systems that uphold academic integrity requirements.

2.13 Hardware Resources Standards

FWU maintains standardized hardware resources, including computers, servers, networking equipment to ensure compatibility, reliability, security, and cost-effectiveness across the IT infrastructure.

2.14 Email System

Users of FWU will have access to official email using the university's domain. Users must use the official email supplied by the university for all official university communications as well as for academic and other purposes.

2.15 Digital Resource Access

FWU is committed to providing secure and authorized access to digital resources, including databases, apps, and online platforms.

2.16 Website Uniformity and Accessibility

To enable an inclusive and user-friendly digital experience for all users while adhering to online accessibility requirements, FWU will maintain uniformity and assure accessibility standards across all of its websites.

2.17 Cloud Infrastructure

In order to increase scalability, flexibility, and cost-efficiency, FWU embraces the use of cloud infrastructure, including Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS), while also ensuring data security, regulatory compliance, and efficient management of cloud-based services and resources.

Institutional Arrangement

3.1 ICT Steering Committee

The university will formulate an ICT Steering Committee as a governance and oversight body to ensure that IT policies and strategies are developed and implemented in a coordinated and effective manner. Moreover, other sub-committees and working groups can be formed as and when needed, in recommendation of the ICT Steering Committee.

3.2 Procurement

While subscribing, acquiring service/equipment, Public Procurement Act 2063, Public Procurement Rules and Regulations and the university's own procurement policy will be followed.

3.3 Formulation of University ICT Master Plan

The formulation of FWU ICT Master Plan will be a collaborative and iterative process. Therefore, FWU will develop its ICT master plan (short-term and long-term strategic planning) through a multi-stage participatory process, involving needs assessment and gap analysis; stakeholder engagement; goal setting and prioritization; resource allocation and budgeting; and implementation and monitoring. The FWU's ICT Master Plan will be developed within a year of the approval of this IT policy.

3.4 Legal and Regulatory Arrangements

There will be a university central level ICT Steering Committee consisting of the following 7 members.

Table 1: University Central Level ICT Steering Committee

SN	Committee Members	Designation
1	Vice-Chancellor	Chair
2	Registrar	Member
3	Rector [Exam Head]	Member
4	Planning Chief	Member
5	Research Director	Member
6	Dean	Member
7	IT Director	Member Secretary

This committee acts as a central regulatory body for IT policy of the university. All other HEI IT policy, strategy, guidelines and procedures will follow this policy guidelines.

FWU will also formulate a subcommittee (under the ICT Steering Committee) to develop a separate guidelines for university e-Governance. The subcommittee will be chaired by the Registrar and will include 7 members, including the following:

Table 2: e-Governance Subcomittee

SN	Committee Members	Designation
1	Registrar	Chair
2	Admin Chief	Member
3	Exam Chief	Member
4	Representative of an Affiliate Campus	Member
5	Dean (Management)	Member
6	Dean (Engineering)	Member
7	IT Director	Member Secretary

3.5 ICT Enabled Monitoring and Evaluation

The IT staff/team and the IT Director are responsible for day-to-day operation and supervision of the IT services. The ICT Steering Committee will conduct an assessment at least once a year; however frequent monitoring of IT services and functions can be done as per committee meeting decisions or as part of redressing IT service-related complaints.

More importantly, the university will adopt ICT enabled monitoring by using some software solutions available for monitoring system performance, network traffic, user experience, security vulnerabilities, and compliance so as to provide real-time monitoring, data visualization, and reporting capabilities. The university will automate the data collection as much as possible to minimize manual effort and improve efficiency. And then, the reports will be shared with decision-makers, IT management, and other relevant stake holders. Based on the evaluation results, the IT unit will develop action plans and implement necessary changes to enhance system performance, security, user experience, and compliance.

3.6 Policy Update and Dissimilation

The University's IT policy will be aligned with the FWU's overall goals and priorities, and will be regularly reviewed (preferably every year) and updated (at least in every five years) to ensure that they remain relevant and effective in a rapidly changing IT landscape. The ICT Steering Committee or an intendent external agency will facilitate the policy update. The updated policy will be shared among the university stakeholders. The final policy document will be uploaded on the university website for wider dissemination and use.

University Digitalization Strategy

4.1 Connectivity

4.1.1 FWU will invest in a reliable and scalable network infrastructure that can handle the university's connectivity requirements. This includes deploying high-speed wired and wireless networks (broadband Internet Connection, Wi-Fi Zone, Intranet, Extranet etc.) to support the growing demands of users and applications

4.1.2 FWU will regularly update and patch network devices and employ strong encryption protocols to protect data in transit.

4.1.3 FWU will also establish a disaster recovery plan to quickly restore connectivity in the event of a network failure or natural disaster.

4.2 Digital Infrastructure

4.2.1 FWU will maintain robust digital infrastructure including IT support unit with Hardware, Software and establishment of Data Center and connectivity with GIDC/Other sources/Cloud Infrastructure.

4.2.2 FWU will invest in modern hardware, such as servers, storage systems, and networking equipment that can handle increased workloads and provide the necessary computing power and storage capacity.

4.2.3 FWU will embrace virtualization technologies and cloud computing to optimize resource utilization, enhance flexibility, and reduce costs.

4.2.4 By regularly assessing the performance and capacity of the digital infrastructure, FWU will develop a proactive approach to infrastructure upgrades and maintenance.

4.3 Virtual Learning Environment

4.3.1 FWU will identify and select a suitable VLE, LMS, MOOC, or self-paced platform that aligns with the university's educational goals and requirements. Considering scalability, features, user interface, integration capabilities, and support for various learning modalities, it is currently adopting MOODLE platform as a user-friendly VLE.

4.3.2 FWU will provide comprehensive training and support to faculty, staff, and students on effectively utilizing the MOODLE platform.

4.3.3 FWU encourages faculty members to develop and curate high-quality digital content suitable for online and blended learning environments.

4.3.4 FWU will also implement a framework for monitoring and evaluating the effectiveness of the VLE, LMS, MOOCs, or self-paced platforms in achieving learning outcomes.

4.3.5 FWU will provide digital resources and platforms to support students' academic success, career development, and over-all wellbeing. This may include tutoring, virtual students clubs, mental health resources and personalized digital advising.

4.4 Strengthening Web Based EMIS

4.4.1 The policy provisions FWU's own Education Management Information System (EMIS) to manage student and staff data from campuses, departments, faculties.

4.4.2 It may be important to integrate EMIS with other university systems to improve efficiency and reduce data duplication. At least, it will be connected with the UGC EMIS.

4.4.3 FWU will ensure that the EMIS is accessible to staff and administrators across the university. This can be achieved by making it available through a web-based interface or mobile application.

4.4.4 FWU will implement measures to protect the privacy and security of university data stored in the EMIS. This can include encryption, user authentication, and access controls.

4.5 Digital Resource Development and Dissemination

4.5.1 FWU will focus on developing and sharing high-quality digital resources (E-library, digital studio and production, and publication of e-books, audio/video, animation, simulation, and gaming learning materials).

4.5.2 The university will establish a digital library that provides access to online resources such as e-books, journals, and research databases.

4.5.3 FWU will have its own digital resource management system. For this, FWU will invest in high-speed internet, powerful servers, and storage systems that are capable of handling large amounts of digital data. This will ensure that digital resources can be accessed and shared efficiently. Likewise, FWU will invest in software tools that can help with digital resource management, archiving, and dissemination.

4.5.4 The university will create a digital studio equipped with state-of-the-art hardware and software. This studio can be used by students, faculty, and staff to create and edit digital resources such as videos, audio recordings, and images. The digital studio will be connected with LMS/net TV.

4.5.5 FWU will explore partnership opportunities with other organizations to develop and disseminate digital resources. This may include joint projects, sharing of resources, and collaborative research initiatives.

4.6 Human Resource Capacity Development

4.6.1 FWU encourages the use of ICT for capacity development, enabling personnel to acquire new skills and knowledge, improve their performance, and enhance their effectiveness.

4.6.2 The e-Governance committee will develop a dedicated IT training portal. The committee conducts needs assessment of the staff and faculty and provides relevant IT training. Moreover, some exchange (student/faculty/staff mobility) programs will also be explored so as to capacitate them. Likewise, further coordination and collaboration with other agencies for capacity development will be done by the HRD.

4.6.3 The university will provide training programs to help students, faculty, and staff learn how to use digital resource management, archiving, and dissemination tools. This may include workshops, online courses, and one-on-one training sessions.

4.6.4 FWU promotes virtual conferencing tools to facilitate virtual training, webinars, and meetings. This can help personnel to collaborate with colleagues and attend professional development events without the need for travel.

4.6.5 FWU also leverages social media platforms to connect personnel with colleagues in their field and stay up-to-date with the latest news and trends.

4.7 University and its campus office automation and EMIS

4.7.1 FWU will implement a comprehensive system automation strategy including for admissions, registration, student records, finance, and human resources, and integrate them into a centralized system.

4.7.2 FWU will deploy a robust Education Management Information System (EMIS) to efficiently collect, manage, and analyze educational data. The EMIS will be aligned with UGC's network.

4.7.3 FWU will gradually establish an e-governance framework that enables efficient decision-making, transparency, and accountability across the university. Implement online portals, digital workflows, and automated approval processes to streamline administrative tasks, improve communication, and enhance service delivery.

4.7.4 Aligning the university's digital strategy with AI involves integrating AI technologies and principles into the strategy to enhance various aspects of the institution's operation and services. AI can be incorporated for:

- Personalized learning
- Intelligent virtual assistance
- Productive analytics
- Research and data analysis
- Intelligent data management
- Smart campus and campus facilities management
- Natural language processing

4.8 University Intellectual Property Security, Privacy, Plagiarism System, Surveillance and Copyright Law

4.8.1 FWU will establish protocols and measures (e.g. access controls, encryption, and data loss prevention mechanisms to safeguard sensitive research findings, patents, copyrights, and trademarks) to protect intellectual property within the university.

4.8.2 FWU will educate faculty, staff, and students about intellectual property rights and the importance of respecting and preserving them.

11

4.8.3 FWU will implement appropriate security measures, such as data encryption, secure data storage, and user authentication protocols to ensure the privacy and protection of personal data.

4.8.4 FWU will implement a robust plagiarism detection system (a paid software) to discourage and identify instances of academic dishonesty.

4.8.5 FWU will provide faculty and students with tools and training to understand plagiarism, cite sources correctly, use copyrighted materials responsibly, and utilize proper research methodologies.

4.8.6 FWU will also establish clear consequences and educational interventions to address instances of plagiarism.

4.8.7 FWU will educate faculty, staff, and students about copyright infringement risks and the importance of obtaining appropriate licenses for using copyrighted content.

4.9 University Data Management, Protection, Back up and Disaster Recovery

4.9.1 The policy provisions FWU's own data backup and disaster recovery system. Currently, FWU's data backup will use the data center of UGC, MoEST and Nepal Government. The university will have its own data center in coming future with a dedicated backup and recovery system.

4.9.2 The IT Director will ensure that regular backups are taken of the university data, including both on-premises and cloud-based data. These backups will be stored securely and regularly tested to ensure that they can be recovered in the event of an outage or disaster.

4.9.3 The university will leverage cloud-based backup solutions to protect its data, including offsite backup and disaster recovery solutions that can provide automatic failover in the event of an outage.

4.9.4 The university will ensure that its backup and disaster recovery systems are secure and that only authorized personnel have access to them. This can include encryption, access controls, and regular security audits.

4.9.5 FWU will have measures in place to prevent, detect, and respond to IT security incidents.

4.10 IT System Security, Safety, Avoidance and Prevention from Attack

4.10.1 FWU though its IT department will conduct regular risk assessments (such as security updates, patch management, and proactive monitoring for emerging threats) to identify potential security vulnerabilities and assess the level of risk.

4.10.2 Implement strong access controls and user authentication mechanisms (such as enforcing strong password policies, implementing two-factor authentication, utilizing role-based access controls, deploying firewalls) to ensure that only authorized individuals can access sensitive data and systems.

12

4.10.3 FWU will regularly conduct security awareness training for faculty, staff, and students to educate them about common cyber threats, phishing attacks, and social engineering techniques.

4.10.4 FWU will develop an incident response system to effectively respond to cyber-attacks and minimize the impact on the university's systems and data.

4.10.5 FWU will regularly communicate security updates and best practices to the university community.

4.11 Cloud-Based Technology for Information Management

4.11.1 FWU promotes the use of cloud-based infrastructure, including Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS)

4.11.2 FWU promotes the use of cloud-based storage solutions such as Google Drive, One Drive, or Drop box to store and share files securely. This can help to reduce the need for physical storage space and make it easier for personnel to access files from anywhere.

4.11.3 The university will increasingly use cloud-based collaboration tools such as Google Docs, Microsoft Teams, or Slack to enable more effective collaboration between personnel. This can include real-time document editing, chat functions, and project management tools.

4.11.4 The university will provide training and support to personnel to ensure that they are able to use cloud-based technology effectively and securely. This can include online training modules, one-on-one coaching, and regular updates on new features and security best practices.

4.12 ICT Enabled Monitoring and Evaluation System

4.12.1 FWU will use ICT to support resource planning and management processes, such as budgeting, procurement, and inventory management. While planning and budgeting, needs assessment of campuses, faculty and university will be done using digital tools. This data can be used to inform university planning and decision-making processes.

4.12.2 FWU will gradually use ICT to monitor performance metrics and indicators related to university operations, such as student retention rates, graduation rates, and research productivity. The university will develop its own monitoring and evaluation system supported by digital technology so as to monitor and track progress and activities through virtual tools and applications.

4.12.3 The IT Director will monitor the use of EMIS to ensure that it is being used effectively and that data is being entered accurately.

4.12.4 FWU will gradually use ICT to evaluate the effectiveness and impact of various initiatives and programs like e-learning programs, student support services, and research centers. This can help identify successful strategies and best practices that can be replicated and scaled up, as well as areas where improvements may be needed.

13

4.12.5 FWU will automate the data collection as much as possible to minimize manual effort and improve efficiency. And then, the reports will be shared with decision-makers, IT management, and other relevant stakeholders.

4.12.6 Based on the evaluation results, the IT unit will develop action plans and implement necessary changes to enhance system performance, security, user experience, and compliance.

Implementation Mechanism

5.1 Implementation Plan with Action Items

SN	Action Items	Timelines	Responsible	Resource Requirements	Milestones
1	Assess the current IT infrastructure and identify necessary upgrades or enhancements.	July 15, 2023	IT Director/ IT Staff	Consultation meetings	Assessment report and action plan
2	Develop training programs to enhance digital literacy and ensure that administrators, faculty, staff, and students have the necessary skills to comply with the policy.	Aug 30, 2023	ICT steering committee/ IT Director/ IT Staff/ External Experts	Multiple rounds of workshops and meetings	Training curricula
3	Provide specialized training sessions for IT administrators, faculty, staff, and students.	One group each month, starting August 2023	IT Director/ IT Staff/ External Experts	Training materials and logistics	Trained administrators, faculty, staff and students
4	Provide comprehensive training and support to faculty on effectively utilizing the MOODLE platform	Before the start of next session	IT Director/ IT Staff/ External Experts	Training materials and logistics	Trained faculty
5	Install Education Management Information System (EMIS) to manage student and staff data from campuses, departments, faculties (follow UGC guidelines)	By the end of 2023	E-Governance subcommittee/ IT Director/ IT Staff	Procurement	EMIS installed
6	Initiate a digital library	November 2023	ICT steering committee/ IT Director	Library hall/building, repository and e-resources	Basic infrastructure and HR managed

7	Develop a dedicated IT training portal	By the end of 2023	IT Director/ IT Staff/ External Experts	Web	Training portal
8	Explore partnership opportunities with other organizations to develop and disseminate digital resources	Continuously	ICT steering committee/ subcommittees/ IT Director	Communication and meetings	Partnership agreements
9	Educate faculty, staff, and students about intellectual property rights and the importance of respecting and preserving them	By September	IT Director/ IT Staff/ External Experts	Training materials and logistics	Trained faculty, staff and students
10	Regularly review progress, gather feedback from stakeholders and make necessary adjustments	Continuously (every three months)	IT Director/ IT Staff	Consultation meetings and online feedback system	Progress reports and action plans
11	Develop a data backup and disaster recovery plan	By the end of 2023	ICT steering committee/ subcommittees/ IT Director	Consultation meetings and workshops	Plan
12	Install a robust plagiarism detection tool/software	By the end of 2023	IT Director/ IT Staff	Software subscription	Plagiarism detection software installed
13	Develop an incident reporting and response system	By the end of 2023	IT Director/ IT Staff	Online system	System in place

5.2 Resources Arrangement and Allocation

5.2.1 For better planning and prioritization of IT resources, specific funds will be allocated annually for IT initiatives aligned with the policy.

5.2.2 While acquiring IT resources, government sources and partnerships will be prioritized. This can involve joint ventures or outsourcing of IT services.

5.2.3 FWU collaborates with other institutions to pool resources and expertise.

5.2.4 FWU will explore grant opportunities and collaborative projects to fund and support its IT initiatives.

5.2.5 FWU can accept donations of IT resources from alumni, corporations, and other benefactors. This can include equipment, software licenses, and funding for IT initiatives.

5.2.6 FWU will optimize the use of existing resources by implementing best practices in IT resource management, including regular maintenance and upgrades, effective use of software licenses, and efficient use of network bandwidth.

5.2.7 FWU will enhance the practice of resource sharing (data center from the university will be shared with faculties).

5.2.8 The IT Director will coordinate and facilitate in supporting campuses and faculties in technology integration issues

5.2.9 FWU students (with computer specialization) will be used as interns to support university IT resource mobilization. Scholarship recipient students can also be mobilized so as to maximize the utilization of IT resources.

5.2.10 IT resources will gradually be expanded to accommodate the increasing number of students and staff. The IT systems will be compatible for further updates.

5.3 Institutional Arrangement

As outlined in the IT policy above, the overall regulatory body of the IT policy and system will be an IT Steering Committee. Under the committee, several subcommittees and units, offices, or task forces can be formed, e.g. e-Governance Subcommittee.

Moreover, the existing IT Department will be responsible for managing and coordinating the implementation of the IT policy and strategy. This Department will provide guidance, support, and expertise in IT policy implementation and compliance. It also serves as a central point of contact for addressing IT policy-related matters.

5.4 Risk Planning and Management

FWU will conduct a thorough risk assessment specific to the implementation of the IT policy.

Assumptions	Risks
The policy assumes that all students and staff have access to technology and the reliable internet.	May not be the case for some as assumed, due to the geographical location of the Province/s (student cover area),internet connectivity and penetration, and socio-economic conditions of the students
The policy assumes that all users have a certain level of technological competence.	This may not be true for everyone.
The policy assumes that the university has sufficient funds to implement and maintain the necessary infrastructure and software, and support end-users.	If funding is cut or not allocated appropriately, this could result in insufficient resources to meet the needs of users.
The policy assumes that backups and	If backups and recovery procedures are not

recovery procedures are in place.	effective, the loss of important data could have serious consequences.
The policy assumes that the technology being used will remain relevant and functional for the foreseeable future.	Technology can change rapidly, and the university may be at risk of investing in systems that quickly become outdated.
The policy assumes that all users are aware of the potential security risks associated with using technology and take appropriate measures to protect their data and the university's data.	With the increasing amount of sensitive data stored on university servers, the risk of a security breach is high.

FWU will then assess the potential impact of identified risks on the implementation of the IT policy. IT will further identify risk mitigation strategies (such as prevention, mitigation, transfer, or acceptance of risks) based on the assessment of each risk. By informing the identified risks, mitigation strategies, and controls to all relevant stakeholders, it will implement appropriate technical controls, such as firewalls, intrusion detection systems, encryption, access controls, and vulnerability patching. Finally, it will regularly monitor the effectiveness of risk mitigation measures and controls.

Information Technology Policy and Strategy 2023

Far Western University
+977-099-520729
info@fwu.edu.np
Bheemdatta Municipality-18, Mahendranagar, Kanchanpur