

ABUBAKAR TAFAWA BALEWA UNIVERSITY, BAUCHI



INFORMATION & COMMUNICATION TECHNOLOGY (ICT) POLICY



© [2021] Abubakar Tafawa Balewa University, Bauchi. All rights reserved.

The ICT Policy of Abubakar Tafawa Balewa University, Bauchi, including all its contents and associated materials, is protected by copyright law. The university holds the copyright to this policy document.

No part of this ICT Policy may be reproduced, distributed, or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without the prior written permission of Abubakar Tafawa Balewa University.

Requests for permissions or inquiries regarding the use of the content of this ICT Policy should be addressed to:

**The Director,
Directorate of Information and Communication Technology,
Abubakar Tafawa Balewa University,
P. M. B., 00248, Bauchi**

Any unauthorized use, reproduction, or distribution of this policy or its contents may result in legal action. Abubakar Tafawa Balewa University reserves the right to enforce its copyright to the fullest extent of the law.

This copyright statement is applicable to all versions and formats of the ICT Policy, including printed and electronic copies, and any future revisions or updates.

[2021] Abubakar Tafawa Balewa University, Bauchi

Creators: ATBU, ICT Directorate

Year: 2021-2025

License Condition: [Full Copyright - All rights reserved](#)

Type: Policy Documents

Section: OER policies in Africa

Publisher/Source: Directorate of Communication and Information Technology, ATBU, Bauchi



ABUBAKAR TAFAWA BALEWA UNIVERSITY, BAUCHI

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

DIRECTORATE OF INFORMATION AND COMMUNICATION TECHNOLOGY

Foreword

It is with great pleasure and a sense of forward-looking anticipation that I introduce the Information and Communication Technology (ICT) Policy of Abubakar Tafawa Balewa University (ATBU), Bauchi. In an era defined by the transformative power of technology, this policy serves as a guiding compass, charting our course toward a future where the seamless integration of ICT elevates the academic, research, and administrative landscape of our esteemed institution.

As the world undergoes a digital revolution, universities play a pivotal role in preparing individuals for the challenges and opportunities that lie ahead. Recognizing this, the ICT Policy of ATBU has been meticulously crafted to embrace the principles of innovation, inclusivity, and sustainability. It reflects our commitment to fostering a technologically empowered environment that nurtures learning, encourages research excellence, and ensures efficient administrative processes.

This policy is more than a set of rules and guidelines; it is a testament to our dedication to providing a dynamic and responsive infrastructure that meets the evolving needs of our academic community. It outlines strategies for infrastructure development, capacity building, and information security, laying the foundation for a robust and resilient ICT ecosystem.

As we embark on this transformative journey, it is essential to acknowledge the collaborative efforts of stakeholders, including faculty, staff, students, and administrators. Their insights and commitment have been instrumental in shaping a policy that not only aligns with global best practices but also encapsulates the unique ethos of ATBU.

Through the implementation of this policy, we envision an environment where digital literacy flourishes, where e-learning

In the pursuit of excellence, the university acknowledges that technology is a dynamic force, and this ICT policy serves as a living document that evolves in tandem with the changing ICT landscape. The commitment to continuous improvement, stakeholder engagement, and transparent communication underscores the university's dedication to creating an ICT environment that not only meets the present needs but anticipates and addresses future challenges.

In essence, this ICT policy stands as a testament to Abubakar Tafawa Balewa University's vision for a digitally enabled future—one where technology enriches the academic experience, safeguards sensitive information, and empowers individuals to harness the transformative potential of the digital era. Through collective adherence to these principles, the university community contributes to a vibrant, secure, and forward-looking ICT ecosystem that reflects the values of Abubakar Tafawa Balewa University.

In concluding the ICT policy for Abubakar Tafawa Balewa University, it is evident that the institution is steadfast in its commitment to fostering a secure, innovative, and ethically responsible digital environment. The comprehensive policies and guidelines outlined herein are designed to empower the university community—comprising students, faculty, staff, and other stakeholders—with the knowledge and tools necessary to navigate the ever-evolving landscape of technology and cybersecurity.

The primary objective of this ICT policy is to create an ecosystem that promotes academic excellence, protects sensitive information, embraces digital innovation, and ensures the responsible and efficient use of ICT resources. By prioritizing data security, privacy, and compliance with relevant laws and standards, the university seeks to establish itself as a trusted custodian of information, upholding the principles of integrity, confidentiality, and availability.

The governance and compliance framework articulated in this policy underscores the importance of robust oversight and accountability. Through periodic reviews, inclusive revision processes, and continuous monitoring, the university aims to adapt swiftly to changes in technology, legal requirements, and emerging cyber threats. This commitment to agility and responsiveness positions Abubakar Tafawa Balewa University at the forefront of technological stewardship.

As the university community engages with this ICT policy, it is crucial to recognize the shared responsibility for the ethical use of ICT resources. Users are not only recipients of the benefits of technology but also stewards of its responsible and secure application. The emphasis on security awareness, training programs, and clear communication channels ensures that every member of the university community is well-informed and equipped to contribute to a culture of cybersecurity and digital citizenship.

becomes an integral part of our educational landscape, and where cutting-edge research is facilitated by state-of-the-art ICT resources. We also emphasize the importance of sustainable ICT practices, ensuring that our technological advancements align with our responsibility to the environment.

In conclusion, I extend my gratitude to all who have contributed to the development of this ICT Policy. May it serve as a catalyst for positive change, innovation, and academic excellence at Abubakar Tafawa Balewa University, propelling us into a future where the transformative potential of technology is harnessed for the greater good.

Prof. Muhammad Ahmad Abdulazeez
Vice Chancellor
Abubakar Tafawa Balewa University, Bauchi

Acknowledgments

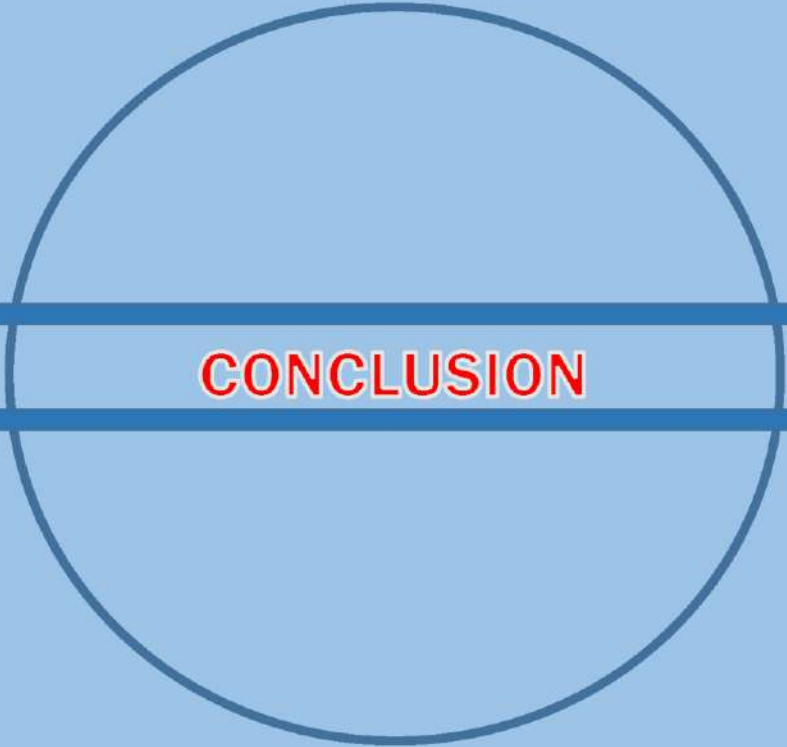
The development and implementation of the Information and Communication Technology (ICT) Policy for Abubakar Tafawa Balewa University (ATBU), Bauchi, have been a collaborative effort that would not have been possible without the dedication, expertise, and support of various individuals and groups.

We extend our sincere appreciation to the Vice-Chancellor, Prof. Muhammad Ahmad Abdulazeez, for providing visionary leadership and unwavering support throughout the formulation of this policy. Your commitment to advancing technological integration in our academic institution has been a driving force behind the establishment of this comprehensive ICT framework.

Our gratitude extends to the ICT Committee, chaired by Professor Ibrahim Mohammed Danjuma, for their tireless efforts in researching, drafting, and refining the policy document. The collective expertise and diverse perspectives contributed by the committee members have ensured that the policy reflects the needs and aspirations of the entire university community.

We also want to express our appreciation to the faculty members, staff, and students of ATBU who actively participated in consultations, workshops, and feedback sessions. Your insights and constructive feedback have been invaluable in shaping a policy that is both pragmatic and forward-thinking.

Special thanks to Prof. I. H. Garba, Prof. S. D. Abdul, Prof. Fatima Sawa, Prof. Balarabe Yusha'u and Prof. Babawuro Shuaibu, for their technical expertise in drafting and refining the language of the policy. Their commitment to clarity and precision has enhanced the accessibility of the document for all stakeholders.



CONCLUSION

commitments of Abubakar Tafawa Balewa University in its approach to information and communication technology (ICT). Here's an expanded conclusion:

We acknowledge the contributions of DICT administrative staff who played a crucial role in coordinating the logistics, communication, and documentation associated with the development of the ICT policy.

Finally, we recognize the broader ATBU community—alumni, parents, and partners—who continue to support our endeavors in advancing education, research, and administration through the effective use of information and communication technology.

This ICT Policy stands as a testament to the collaborative spirit and shared vision of the ATBU community. Together, we look forward to a future where technology enhances our educational mission and contributes to the continued growth and excellence of Abubakar Tafawa Balewa University, Bauchi.

Prof. Abdulsalam Ya'u Gital
Ag. Director, DICT,
Abubakar Tafawa Balewa University, Bauchi

Table of Contents

Contents	Page
Foreword	-2
Acknowledgements	-4
Table of Contents	-6
List of abbreviations	-7
Executive Summary	-8
Definition of Terms	-10
1. Introduction	-13
1.1 Purpose	-14
1.2 Scope of the Policy	-16
2. Acceptable Use of ICT Resources	-20
2.1 Responsible Use	-21
2.2 Prohibited Activities	-21
2.3 Personal Use Guidelines	-23
2.4 Consequences of Non-Compliance	-23
3. Data Security and Privacy	-24
3.1 Data Protection	-25
3.2 Privacy	-26
3.3 Incident Response	-27
3.3 Monitoring & Auditing	-27
4. ICT Infrastructure Management	-28
4.1 Network Access	-29
4.2 Device Management	-29
4.3 Server & Database Management	-30
4.4 Cloud Services Management	-31
4.5 Disaster Recovery & Business Continuity	-31
4.6 Environmental Sustainability	-32
5. Cybersecurity	-33
5.1 Security Awareness	-34
5.2 Security Policies & Procedures	-34
5.3 Incident Response	-35
5.4 Access Controls	-35
5.5 Security Technologies	-36
5.6 Security Monitoring and Threats Intelligent	-36
5.7 Security Reviews and Audits	-37
5.8 Collaboration and Communication	-37
6. Governance and Compliance	-39
6.1 ICT Governance Structure	-40
6.2 Policy Development and Review	-40
6.3 Compliance Framework	-41
6.4 Risk Management	-41
6.5 Accountability and Transparency	-42
6.6 Continuous Improvement	-42
7. Review and Revision	-44
7.1 Periodic Review	-45
7.2 Revision	-45
7.3 Inclusive Revision Process	-46
7.4 Communication	-47
7.5 Documentation	-47
Conclusion	-49

clear communication channels, targeted messaging, and awareness campaigns to ensure that all stakeholders are well-informed about the changes and the reasons behind them.

7.4.2 Training and Education

Training sessions and educational resources will be provided to facilitate understanding and compliance with the revised policy. This includes training programs on new security measures, changes in acceptable use guidelines, and any other aspects of the policy that may impact users.

7.5 Documentation

7.5.1 Documenting Revisions

All revisions to the ICT policy will be thoroughly documented. This documentation will include the rationale for changes, feedback received, impact assessments, and the version history of the policy. Maintaining clear and accessible records ensures transparency and accountability in the revision process.

7.5.2 Accessibility of Policy Documents

Revised policy documents will be made easily accessible to all members of the university community. This includes publishing the latest version on the university's website, distributing printed copies as necessary, and ensuring that users can easily reference and access the policy when needed.

Certainly, expanding on the conclusion provides an opportunity to summarize the key points and emphasize the overarching goals and

7.2.2 Continuous Monitoring

A continuous monitoring mechanism will be in place to track developments in the ICT landscape. This includes staying informed about emerging cybersecurity threats, technological innovations, and changes in the legal and regulatory environment. Regular updates will be made to the policy in response to these developments.

7.3 Inclusive Revision Process

7.3.1 Collaboration and Consultation

Revision processes will emphasize collaboration and consultation with stakeholders across the university community. Workshops, focus groups, and open forums will be conducted to gather insights, concerns, and recommendations from various perspectives. This inclusive approach ensures that the revised policy reflects a collective understanding and commitment to its principles.

7.3.2 Impact Assessment

Before implementing revisions, the potential impact of changes on different stakeholders and university operations will be assessed. This impact assessment will consider factors such as usability, accessibility, and the ability of users to comply with the updated policy. Efforts will be made to minimize disruptions and facilitate a smooth transition to the revised policy.

7.4 Communication

7.4.1 Communication Plan

A communication plan will be developed to inform the university community about upcoming policy revisions. This plan will include

List of abbreviations:

1. **ICT:** Information and Communication Technology
2. **IT:** Information Technology
3. **ATBU:** Abubakar Tafawa Balewa University
4. **DICT:** Directorate of Information and Communication Technology
5. **EDR:** Endpoint Detection and Response
6. **MDM:** Mobile Device Management
7. **SIEM:** Security Information and Event Management
8. **MFA:** Multi-Factor Authentication
9. **BYOD:** Bring Your Own Device
10. **PII:** Personally Identifiable Information
11. **Wi-Fi:** Wireless Fidelity
12. **ISO:** International Organization for Standardization
13. **GDPR:** General Data Protection Regulation
14. **HTTPS:** Hypertext Transfer Protocol Secure
15. **URL:** Uniform Resource Locator
16. **LAN:** Local Area Network
17. **WPA2:** Wi-Fi Protected Access 2
18. **ISP:** Internet Service Provider
19. **FTP:** File Transfer Protocol
20. **IP:** Intellectual Property

Executive Summary

Introduction: Abubakar Tafawa Balewa University, Bauchi, Nigeria, is committed to establishing and maintaining a comprehensive Information and Communication Technology (ICT) policy. This executive summary provides an overview of the key components and objectives outlined in the university's ICT policy.

Purpose: The ICT policy is crafted to provide a framework for responsible and secure technology use within the university community. It aligns with the institution's mission to foster academic excellence, innovation, and ethical conduct in the digital age. The policy aims to ensure the confidentiality, integrity, and availability of information while promoting a collaborative and technologically advanced environment.

Scope: The policy's scope is broad, encompassing all members of the university community, ICT devices and equipment, networks and systems, academic and administrative functions, and compliance with legal and regulatory requirements. It addresses the dynamic nature of technology, ensuring adaptability to emerging trends and challenges.

Key Components:

1. Acceptable Use of ICT Resources: Defines ethical conduct, professionalism, and compliance with policies. Outlines prohibited activities and establishes consequences for non-compliance.

2. Data Security and Privacy: Focuses on data protection, encryption, access controls, and incident response. Emphasizes privacy considerations, data minimization, and legal compliance.

3. ICT Infrastructure Management: Covers network security, device management, server and database security, cloud services management, disaster recovery, and environmental sustainability.

7.1 Periodic Review

7.1.1 Frequency of Reviews

To ensure the continued relevance and effectiveness of the ICT policy, a periodic review process will be established. The frequency of reviews will be defined based on the pace of technological advancements, changes in the regulatory landscape, and emerging cybersecurity threats. A schedule for reviews, at minimum annually, will be adhered to, with the flexibility to conduct ad-hoc reviews as needed.

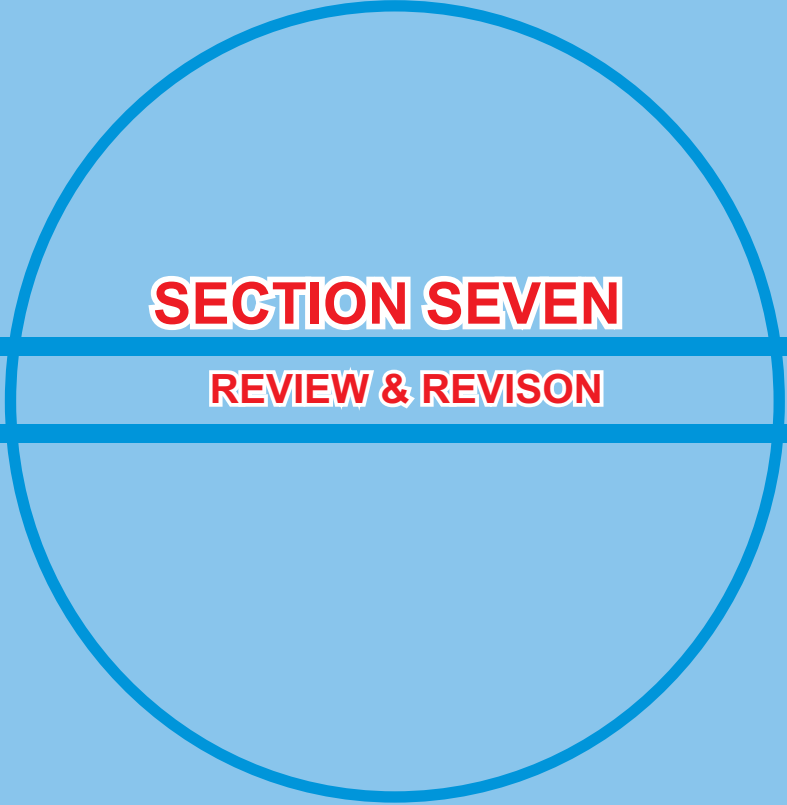
7.1.2 Stakeholder Involvement

The review process will involve active participation from a diverse range of stakeholders, including representatives from academic departments, administrative units, cybersecurity experts, legal advisors, and relevant external entities. Feedback from the university community will be solicited to ensure that the policy reflects the evolving needs and perspectives of users.

7.2 Revision

7.2.1 Trigger Events for Revisions

Revisions to the ICT policy may be triggered by significant changes in technology, amendments to relevant laws and regulations, major cybersecurity incidents, or advancements in best practices. Additionally, feedback from stakeholders, the outcomes of risk assessments, and lessons learned from security incidents will contribute to the identification of areas for improvement.



SECTION SEVEN

REVIEW & REVISION

4. Cybersecurity: Addresses security awareness, policies and procedures, incident response, access controls, security technologies, security monitoring, threat intelligence, and security reviews.

5. Governance and Compliance: Establishes ICT governance structures, policy development and review processes, compliance frameworks, risk management, accountability, transparency, and continuous improvement.

6. Review and Revision: Emphasizes periodic reviews, inclusive revision processes, continuous monitoring, stakeholder involvement, effective communication, training, and comprehensive documentation.

Conclusion: The ICT policy concludes with a firm commitment to creating a dynamic and responsive digital environment. It highlights the university's dedication to excellence, adaptability, and collective responsibility for the ethical and secure use of ICT resources. Through periodic reviews, stakeholder engagement, and continuous improvement initiatives, Abubakar Tafawa Balewa University strives to be at the forefront of technological stewardship.

Recommendation: All members of the university community are urged to familiarize themselves with the ICT policy, adhere to its principles, and actively contribute to the cultivation of a secure, innovative, and ethically sound digital ecosystem. The policy is a living document, evolving in tandem with technological advancements and the evolving needs of the university community.

DEFINITION OF TERMS

These definitions are provided to clarify and establish a common understanding of key terms used throughout the ICT Policy document.

Acceptable Use

The ethical and authorized utilization of ICT resources within the university, encompassing proper conduct, policy adherence, and lawful engagement with technology.

BYOD (Bring Your Own Device)

The practice permitting members of the university community to use their personal devices for academic and administrative purposes, subject to specified guidelines.

Cloud Services

ICT resources and applications delivered over the internet, including storage, processing, and software services hosted on remote servers.

Cybersecurity

The practice of safeguarding ICT systems, networks, and data from unauthorized access, cyber threats, and malicious activities.

Data Governance

The framework and processes ensuring the effective management, integrity, and security of data throughout its lifecycle within the university.

6.6.2 Feedback Mechanisms

A feedback mechanism will be established to gather input from the university community on the effectiveness of ICT governance and compliance efforts. This feedback will inform continuous improvement initiatives, ensuring that the governance framework evolves in response to changing needs and challenges.

6.4.2 Mitigation Strategies

Mitigation strategies will be developed and implemented to address identified risks. These strategies may include technical controls, process improvements, and training initiatives to reduce the likelihood and impact of potential risks.

6.5 Accountability and Transparency

6.5.1 Reporting Mechanisms

Clear reporting mechanisms will be established to ensure accountability at all levels of ICT governance. This includes mechanisms for reporting compliance violations, security incidents, and progress in implementing risk mitigation strategies.

6.5.2 Transparency in Decision-Making

Decisions made by ICT governance bodies will be transparent and well-documented. Stakeholders will be informed of key decisions, policy changes, and any other relevant information through accessible communication channels.

6.6 Continuous Improvement

6.6.1 Performance Monitoring

Performance indicators and metrics will be defined to monitor the effectiveness of ICT governance structures and compliance efforts. Regular assessments will be conducted to measure progress, identify areas for improvement, and refine governance processes.

Endpoint Security

Measures and technologies implemented to secure individual devices (endpoints) connected to the university network against cyber threats.

Incident Response

The coordinated approach to identifying, managing, and mitigating the impact of ICT security incidents, ensuring a swift and effective response.

ICT Infrastructure

The collective hardware, software, networks, and facilities forming the foundation of the university's information and communication technology ecosystem.

Multi-Factor Authentication (MFA)

A security mechanism requiring users to provide multiple forms of identification before accessing ICT systems, enhancing authentication security.

Network Security

Measures and protocols implemented to safeguard the integrity and confidentiality of data transmitted over the university's computer network.

Patch Management

The systematic process of identifying, deploying, and managing software updates and patches to address vulnerabilities and enhance security.

Server Security

Measures and practices ensuring the protection and integrity of servers hosting university applications, data, and services.

SIEM (Security Information and Event Management)

A comprehensive solution for real-time analysis of security alerts and events generated by network hardware and applications.

Threat Intelligence

Information about potential and current cybersecurity threats, vulnerabilities, and risks that may impact the university's ICT environment.

Wireless Network Security

Security measures and protocols applied to wireless networks to protect against unauthorized access and ensure secure data transmission.

into account changes in technology, legal and regulatory requirements, and emerging cybersecurity threats.

6.3 Compliance Framework

6.3.1 Legal and Regulatory Compliance

The university is committed to adhering to all relevant local, national, and international laws and regulations governing ICT activities. A compliance framework will be established to monitor and ensure alignment with legal requirements related to data protection, privacy, intellectual property, and cybersecurity.

6.3.2 Industry Standards Adherence

The university will align its ICT practices with industry best practices and standards. This includes compliance with international standards such as ISO/IEC 27001 for information security management, ensuring a recognized and robust framework for maintaining the security of information assets.

6.4 Risk Management

6.4.1 Risk Assessment

A comprehensive risk management framework will be established to assess, identify, and prioritize potential risks associated with ICT activities. Risk assessments will consider factors such as data breaches, system failures, and other threats that may impact the university's academic and administrative functions.

6.1 ICT Governance Structure

6.1.1 Establishment of Governance Bodies

Abubakar Tafawa Balewa University recognizes the importance of effective ICT governance and will establish governance bodies responsible for overseeing the development, implementation, and enforcement of ICT policies. These bodies may include an ICT Steering Committee, composed of key stakeholders from academic, administrative, and technical domains.

6.1.2 Roles and Responsibilities

Clear roles and responsibilities will be defined for each governance body, outlining their functions, decision-making authority, and accountability. The governance structure will facilitate collaboration and communication among different university departments, ensuring a holistic approach to ICT management.

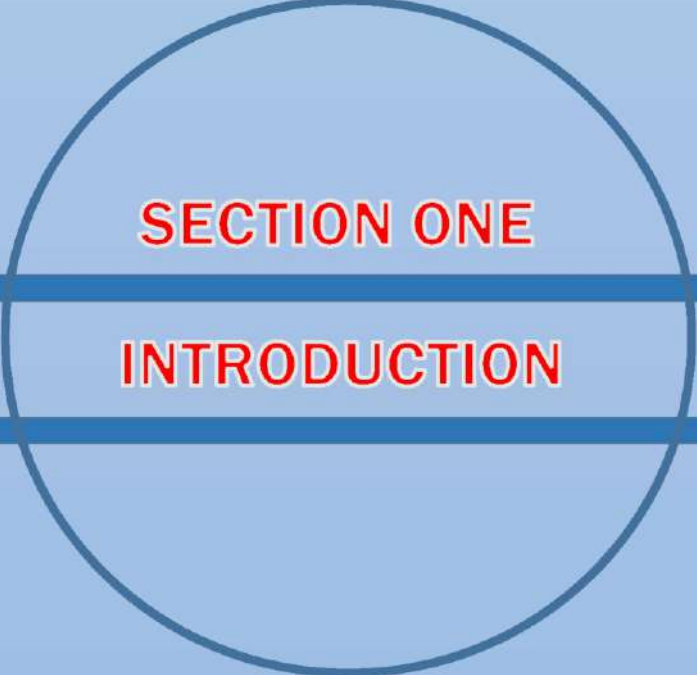
6.2 Policy Development and Review

6.2.1 Policy Development Process

A structured and inclusive process for developing and updating ICT policies will be established. This process will involve soliciting input from relevant stakeholders, conducting impact assessments, and ensuring that policies align with the university's strategic objectives and values.

6.2.2 Regular Policy Reviews

A systematic schedule for policy reviews will be implemented to ensure that ICT policies remain current and effective. Reviews will take



SECTION ONE

INTRODUCTION

Information and Communication Technology (ICT) has become an indispensable tool in today's rapidly evolving global landscape, transforming the way we communicate, access information, and conduct various aspects of our lives. Recognizing the pivotal role that ICT plays in education, research, and administration, Abubakar Tafawa Balewa University (ATBU), Bauchi, is committed to establishing and implementing a comprehensive ICT policy.

The ICT Policy of ATBU is designed to provide a strategic framework that ensures the effective integration, utilization, and management of ICT resources within the university community. This policy aims to foster a conducive environment for academic and administrative excellence, promoting innovation, collaboration, and efficiency through the judicious application of information technology.

1.1 Purpose

1.1.1 Enhancing Academic Excellence

The primary purpose of this ICT Policy is to foster and enhance academic excellence at Abubakar Tafawa Balewa University by providing a framework for the responsible, secure, and efficient use of information and communication technologies. By establishing guidelines for the ethical and effective utilization of ICT resources, the policy aims to support the university's commitment to delivering high-quality education, research, and administrative services.

1.1.2 Ensuring Information Security

In an era where information is a valuable asset, this policy is designed to ensure the security of sensitive and confidential data. By promoting best practices in data protection, encryption, and secure network access, the university aims to safeguard the integrity and confidentiality

SECTION SIX

GOVERNANCE & COMPLIANCE

5.8.2 Communication during Cybersecurity Incidents

In the event of a cybersecurity incident, clear communication channels will be established to keep the university community informed. Transparent and timely communication helps manage the impact of incidents and fosters trust among stakeholders.

of academic and administrative information, protecting the privacy of students, faculty, and staff.

1.1.3 Fostering a Digital Learning Environment

Abubakar Tafawa Balewa University recognizes the transformative power of technology in education. This policy seeks to create an environment that encourages the integration of innovative ICT tools and platforms into teaching and learning processes. By doing so, the university aims to prepare students for the digital era and enhance their competitiveness in a globally connected world.

1.1.4 Mitigating Cybersecurity Risks

As cyber threats continue to evolve, the university is committed to mitigating cybersecurity risks that could compromise the availability, integrity, or confidentiality of its ICT resources. This policy establishes guidelines for cybersecurity awareness, incident reporting, and proactive measures to safeguard against cyber threats, ensuring the resilience of the university's digital infrastructure.

1.1.5 Promoting Responsible Digital Citizenship

Beyond academic and administrative functions, the ICT Policy endeavors to cultivate a culture of responsible digital citizenship among all members of the university community. By defining acceptable use, ethical behavior, and the consequences of non-compliance, the policy encourages users to contribute to a positive and constructive digital environment.

1.1.6 Supporting Operational Efficiency

Efficient and effective ICT utilization is vital for the smooth operation of administrative processes. This policy aims to streamline and optimize the use of ICT resources in administrative functions, enhancing workflow efficiency, reducing redundancy, and improving overall service delivery across the university.

1.2 Scope of ICT Policy

1.2.1 Applicability

1.2.1.1 University Community

This policy applies to all members of the Abubakar Tafawa Balewa University community, including but not limited to students, faculty, staff, researchers, administrators, contractors, and any other individuals granted access to the university's information and communication technology (ICT) resources. It encompasses all levels of users, from novice to expert, emphasizing a collective responsibility for the proper use and protection of ICT assets.

1.2.1.2 Devices and Equipment

The scope includes all computing devices, communication tools, network equipment, and associated peripherals owned, leased, or operated by the university. This covers desktop computers, laptops, tablets, smartphones, servers, routers, switches, and any emerging technologies introduced to the university's ICT ecosystem.

5.6.2 Threat Intelligence Sharing

The university will actively participate in information sharing and collaboration with external cybersecurity organizations, government agencies, and peer institutions to stay informed about the latest threats and vulnerabilities. This collaborative approach enhances the university's ability to proactively defend against emerging cyber threats.

5.7 Security Reviews and Audits

5.7.1 Regular Security Audits

Regular security audits, both internal and external, will be conducted to assess the effectiveness of cybersecurity measures. These audits will evaluate the security of network configurations, applications, and data storage systems, identifying areas for improvement.

5.7.2 Penetration Testing

Periodic penetration testing will be carried out to simulate cyber-attacks and assess the resilience of the university's ICT infrastructure. The results of penetration tests will inform updates to security controls and incident response procedures.

5.8 Collaboration and Communication

5.8.1 Collaboration with External Entities

The university will engage in collaborative efforts with external entities, including law enforcement agencies, cybersecurity organizations, and industry partners, to share information, resources, and best practices in the fight against cyber threats.

5.4.2 Least Privilege Principle

Access to university ICT resources will follow the principle of least privilege. Users will only be granted the minimum level of access necessary to perform their job responsibilities, reducing the risk of unauthorized access and data breaches.

5.5 Security Technologies

5.5.1 Endpoint Security

Endpoint protection solutions, including antivirus software, endpoint detection and response (EDR) tools, and mobile device management (MDM) systems, will be deployed to safeguard against malware, ransomware, and other threats at the device level.

5.5.2 Network Security

Advanced network security measures, such as firewalls, intrusion prevention systems, and secure Wi-Fi protocols, will be implemented to protect against external and internal threats. Regular vulnerability assessments will be conducted to identify and address potential weaknesses.

5.6 Security Monitoring and Threat Intelligence

5.6.1 Continuous Monitoring

Continuous monitoring of network and system activities will be conducted to detect and respond to security incidents in real-time. Security information and event management (SIEM) tools will be utilized to aggregate and analyze log data for signs of malicious activity.

1.2.1.3 Networks and Systems

The policy governs the use of the university's computer networks, servers, databases, software applications, and other information systems. It encompasses both wired and wireless networks, intranet and internet services, cloud-based platforms, and any other infrastructure components that fall within the purview of the university's ICT environment.

1.2.1.4 University Premises and Remote Access

Whether accessing ICT resources on-campus or remotely, users are bound by the guidelines outlined in this policy. Remote access includes connections made through virtual private networks (VPNs), off-campus internet access, and any other means by which individuals interact with university ICT resources from locations outside the physical premises of the institution.

1.2.1.5 Third-Party Relationships

Where applicable, the policy extends to cover third-party vendors, contractors, consultants, and collaborators who have access to the university's ICT infrastructure. All external entities engaging with university ICT resources must adhere to the principles and guidelines set forth in this policy.

1.2.2 Educational and Research Environments

1.2.2.1 Academic Use

The policy addresses the use of ICT resources for academic purposes, including online learning, research, collaborative projects, and any

technology-related activities that contribute to the academic mission of the university.

1.2.2.2 Research and Innovation

It extends to cover ICT resources used in research endeavors, fostering a secure and technologically advanced environment that supports innovation, experimentation, and the pursuit of knowledge.

1.2.3 Administrative and Operational Environments

1.2.3.1 Administrative Functions

The policy governs the use of ICT resources in administrative and operational functions, including but not limited to finance, human resources, student services, and other administrative processes critical to the university's day-to-day operations.

1.2.3.2 Institutional Data

It includes the management and protection of institutional data, covering both academic and administrative data sets, ensuring the integrity, confidentiality, and availability of such information.

1.2.4 Legal and Regulatory Compliance

1.2.4.1 Compliance with Laws and Regulations

This policy ensures compliance with all relevant local, national, and international laws and regulations governing the use of ICT resources, including data protection, privacy, intellectual property, and cybersecurity laws.

addressed through corrective actions and additional training, with a focus on fostering a culture of adherence to security standards.

5.3 Incident Response

5.3.1 Incident Identification

The university will implement robust mechanisms for the early identification of cybersecurity incidents. This includes the use of intrusion detection systems, security information and event management (SIEM) tools, and user reporting systems to detect anomalies and potential security breaches.

5.3.2 Incident Handling

In the event of a cybersecurity incident, a well-defined incident response plan will be activated promptly. This plan will outline procedures for containment, eradication, recovery, and lessons learned. Clear communication channels will be established to keep stakeholders informed during the incident response process.

5.4 Access Controls

5.4.1 Multi-Factor Authentication (MFA)

Multi-factor authentication will be enforced for access to critical systems, applications, and sensitive data. This additional layer of security helps protect against unauthorized access even in the event of compromised passwords.

5.1 Security Awareness

5.1.1 Training Programs

The university will implement comprehensive cybersecurity training programs for all users. These programs will cover the latest cybersecurity threats, social engineering techniques, and best practices for maintaining a secure digital environment. Users will be educated on recognizing phishing attempts, secure password management, and the importance of reporting suspicious activities.

5.1.2 Regular Updates

Cybersecurity training materials will be regularly updated to reflect emerging threats and technologies. Continuous education and awareness campaigns will reinforce the importance of individual responsibility in maintaining a cyber-secure environment.

5.2 Security Policies and Procedures

5.2.1 Policy Development

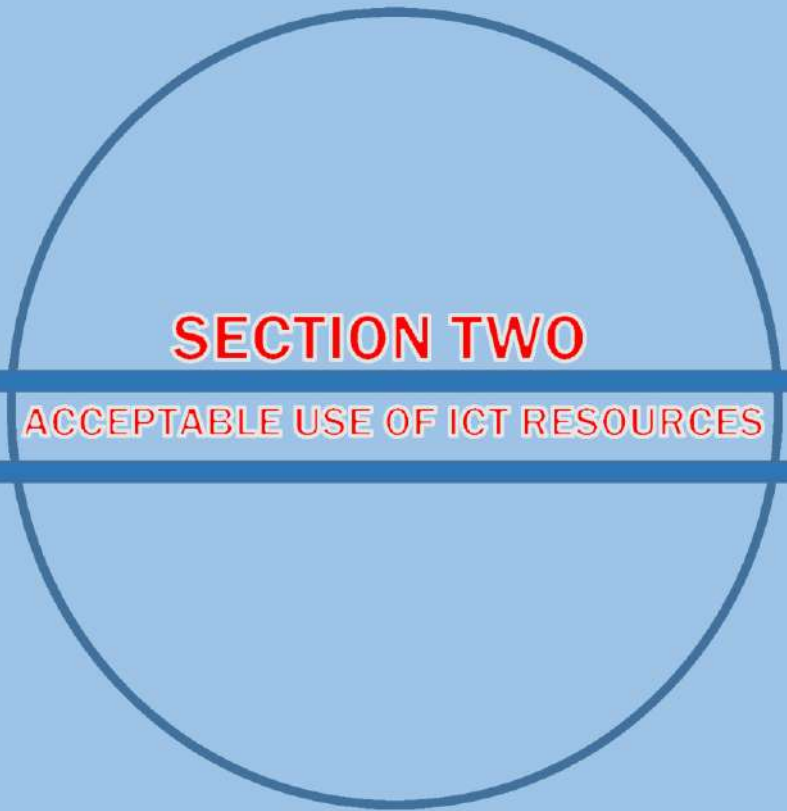
The university will establish and regularly update cybersecurity policies and procedures to address evolving threats. These policies will cover areas such as data classification, access controls, incident response, and acceptable use, providing clear guidelines for the entire university community.

5.2.2 Compliance Monitoring

Regular audits and assessments will be conducted to ensure compliance with cybersecurity policies. Non-compliance will be

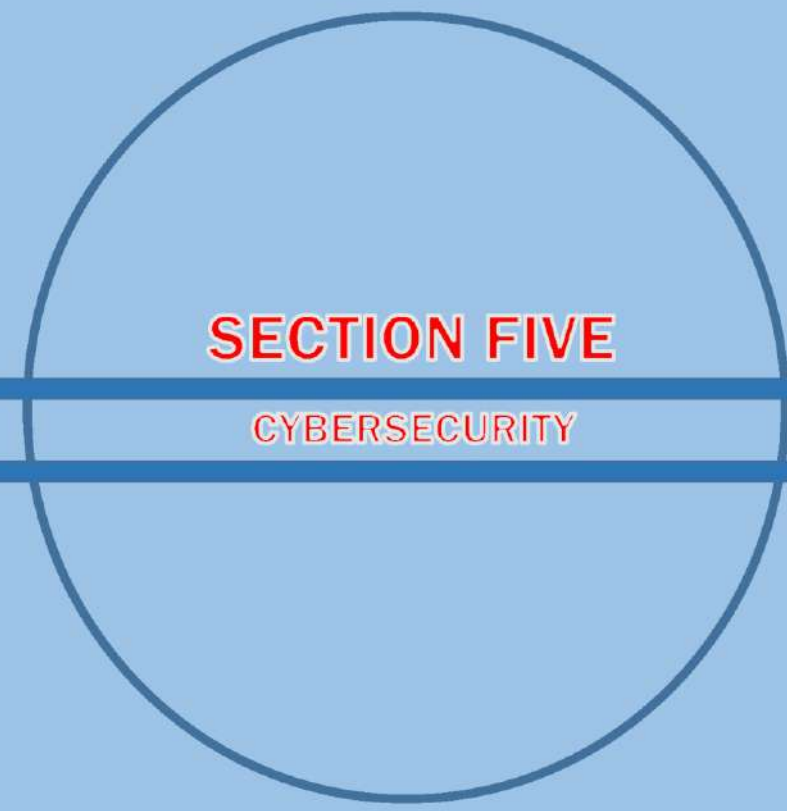
1.2.4.2 Policy Alignment

It aligns with other university policies, ensuring consistency and synergy with policies related to data governance, security, ethics, and acceptable use.



SECTION TWO

ACCEPTABLE USE OF ICT RESOURCES



SECTION FIVE

CYBERSECURITY

4.5.2 Business Continuity

To ensure the continuity of critical university functions, a business continuity plan will be in place. This plan will outline procedures for maintaining essential operations during disruptions and will include provisions for remote work and alternative communication channels.

4.6 Environmental Sustainability

4.6.1 Green ICT Practices

The university is committed to adopting green ICT practices to minimize its environmental impact. This includes energy-efficient configurations, responsible disposal of electronic waste, and promoting awareness of sustainability practices among the university community.

2.1 Responsible Use

2.1.1 Ethical Conduct

Users are expected to engage in ethical and responsible conduct when utilizing university ICT resources. This includes, but is not limited to, respecting the rights and intellectual property of others, avoiding plagiarism, and adhering to the principles of academic integrity in all digital activities.

2.1.2 Professionalism

All members of the university community must conduct themselves professionally in their use of ICT resources, whether engaging in academic research, administrative tasks, or collaborative projects. Professionalism extends to communication, collaboration, and the sharing of digital content.

2.1.3 Compliance with Policies and Regulations

Users are required to comply with this ICT Policy, as well as other relevant university policies and guidelines. Adherence to local, national, and international laws and regulations governing ICT use is mandatory.

2.2 Prohibited Activities

2.2.1 Unauthorized Access

Unauthorized access to computer systems, networks, data, or other ICT resources is strictly **prohibited**. Users must not attempt to bypass security measures, exploit vulnerabilities, or gain access to information for which they do not have explicit authorization.

2.2.2 Distribution of Malware

Engaging in activities that involve the creation, distribution, or use of malicious software, including viruses, worms, trojans, or any other forms of malware, is strictly **prohibited**. Users are responsible for taking measures to prevent the inadvertent spread of malware.

2.2.3 Unauthorized Use of Software and Digital Content

Users must only use software and digital content in compliance with licensing agreements and copyright laws. Unauthorized reproduction, distribution, or use of proprietary software, digital media, or other intellectual property is **prohibited**.

2.2.4 Disruption of ICT Infrastructure

Any action that disrupts or compromises the integrity, availability, or performance of university ICT infrastructure is strictly prohibited. This includes, but is not limited to, intentional network disruptions, overloading systems, or engaging in activities that result in service degradation for others.

2.2.5 Cybersecurity Threats

Users must not engage in activities that pose cybersecurity threats to the university's ICT environment. This includes phishing, social engineering, and any attempt to compromise the confidentiality, integrity, or availability of information.

4.3.2 Database Security

Databases containing sensitive information will be protected through encryption, access controls, and regular monitoring. Database administrators will follow industry best practices to ensure data integrity, confidentiality, and availability.

4.4 Cloud Services Management

4.4.1 Cloud Security

When utilizing cloud services, the university will select providers that adhere to robust security standards. Data stored in the cloud will be encrypted, and access controls will be implemented to safeguard against unauthorized access.

4.4.2 Data Governance in the Cloud

Clear policies and procedures for data governance will be established when using cloud services. This includes defining responsibilities for data management, compliance with data protection laws, and ensuring the secure migration of data to and from the cloud.

4.5 Disaster Recovery and Business Continuity

4.5.1 Disaster Recovery Planning

A comprehensive disaster recovery plan will be established to mitigate the impact of unforeseen events on the university's ICT infrastructure. This includes regular backups, off-site storage of critical data, and the development of recovery procedures for different types of disasters.

antivirus software and endpoint detection and response (EDR) tools, will be implemented to safeguard against malware and other security threats.

4.2.2 Patch Management

Regular and timely updates, including security patches and software updates, will be applied to all devices connected to the university network. An efficient patch management system will be in place to address vulnerabilities and enhance the overall security posture of ICT assets.

4.2.3 Bring Your Own Device (BYOD) Guidelines

If applicable, guidelines for the use of personal devices on the university network (BYOD) will be established. This includes ensuring that personal devices comply with security standards, particularly when accessing sensitive university data.

4.3 Server and Database Management

4.3.1 Server Security

Servers hosting university applications and data will be secured with access controls, encryption, and regular security audits. Only authorized personnel will have administrative access to servers, and remote access will be protected using secure and encrypted connections.

2.3 Personal Use Guidelines

2.3.1 Limited Personal Use

While recognizing the importance of work-life balance, personal use of university ICT resources should be limited and should not interfere with academic or work-related responsibilities. Excessive personal use that impacts network performance or violates other aspects of this policy is not permitted.

2.3.2 Social Media and Online Presence

When using social media and creating an online presence, users should be mindful of representing themselves and the university positively. Posting inappropriate content, engaging in cyberbullying, or using social media in ways that violate the university's code of conduct is not allowed.

2.4 Consequences of Non-Compliance

2.4.1 Disciplinary Actions

Non-compliance with this ICT Policy may result in disciplinary actions, which can include warnings, suspension of ICT privileges, temporary or permanent account suspension, or other measures as deemed appropriate by university authorities.

2.4.2 Legal Consequences

Violations of this policy that involve illegal activities may result in legal action, as well as cooperation with law enforcement authorities.

Users are encouraged to familiarize themselves with this section and adhere to the guidelines outlined to ensure the responsible and ethical use of Abubakar Tafawa Balewa University's ICT resources.

SECTION THREE

DATA SECURITY & PRIVACY

4.1 Network Access

4.1.1 Network Security

The university's computer network is a critical component of its ICT infrastructure. It shall be protected using robust security measures, including firewalls, intrusion prevention systems, and encryption protocols. Access to the network will be controlled through secure authentication mechanisms, and only authorized devices will be permitted to connect.

4.1.2 Wireless Network Security

Wireless networks shall be configured with strong encryption protocols and secure authentication methods. The use of secure, unique passwords for Wi-Fi access will be enforced, and guest networks, if implemented, will be isolated from the main network to prevent unauthorized access.

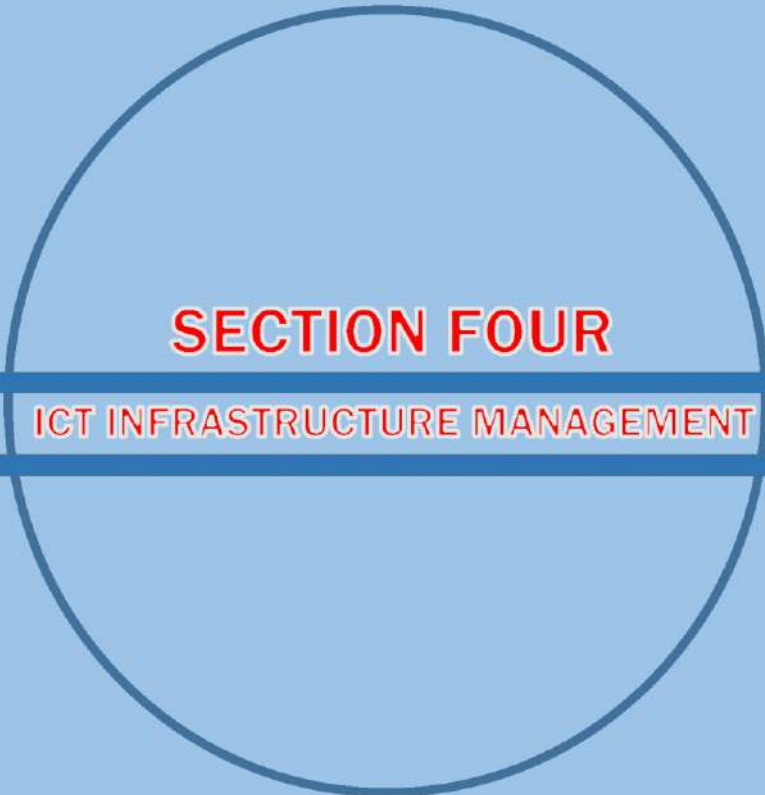
4.1.3 Network Performance

To ensure optimal performance, the university will regularly assess and upgrade its network infrastructure. Bandwidth management strategies will be employed to prioritize academic and administrative activities, preventing network congestion and slowdowns.

4.2 Device Management

4.2.1 Endpoint Security

All devices connected to the university network, including desktop computers, laptops, tablets, and smartphones, shall adhere to established security standards. Endpoint protection solutions, such as



SECTION FOUR

ICT INFRASTRUCTURE MANAGEMENT

3.1 Data Protection

3.1.1 Classification of Data

To ensure appropriate protection, data held within the university's ICT environment shall be classified based on its sensitivity. Categories may include public, internal use only, confidential, and restricted. Users must understand and adhere to the classification of data they handle.

3.1.2 Encryption

Sensitive and confidential information, both in transit and at rest, must be encrypted using industry-standard encryption algorithms. This includes data stored on devices, transmitted over networks, and shared among users.

3.1.3 Data Backups

Regular and secure backups of critical data must be maintained to mitigate the risk of data loss due to accidental deletion, system failures, or other unforeseen events. Backup procedures should be established and periodically tested for reliability.

3.1.4 Access Controls

Access to sensitive data shall be restricted based on the principle of least privilege. Users should only be granted access to the data necessary for their specific roles, and access permissions should be regularly reviewed and updated.

3.2 Privacy

3.2.1 Personally Identifiable Information (PII)

Personally Identifiable Information, such as names, addresses, and identification numbers, should be handled with utmost care. Access to PII should be restricted to authorized personnel only, and its collection, storage, and processing should comply with applicable data protection laws.

3.2.2 Data Minimization

The university encourages the practice of data minimization, wherein only the minimum amount of data necessary for a specific purpose is collected and retained. Unnecessary collection and storage of personal data are to be avoided.

3.2.3 Consent

Where required by applicable laws and regulations, explicit consent must be obtained from individuals before collecting, processing, or sharing their personal information. Consent mechanisms should be transparent, and individuals should be informed of the specific purposes for which their data will be used.

3.2.4 Data Security Awareness

All users with access to sensitive data must undergo regular training on data security and privacy awareness. This includes understanding the risks associated with mishandling data, recognizing social engineering tactics, and staying informed about emerging threats.

3.3 Incident Response

3.3.1 Reporting Security Incidents

Any suspected or confirmed data breaches or security incidents must be reported immediately to the designated ICT security team. Incident response procedures will be activated promptly to investigate, contain, and mitigate the impact of the incident.

3.3.2 Communication

In the event of a data breach, clear and timely communication will be made to affected individuals, regulatory authorities, and other stakeholders in accordance with applicable laws and regulations.

3.4 Monitoring and Auditing

3.4.1 Continuous Monitoring

The university will implement continuous monitoring mechanisms to detect and respond to security incidents promptly. This includes the use of intrusion detection systems, log analysis, and other tools to monitor network and system activities.

3.4.2 Regular Audits

Periodic security audits and assessments will be conducted to evaluate the effectiveness of data security measures, identify vulnerabilities, and ensure compliance with this policy and relevant regulations.