INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

BIKSHU UNIVERSITY OF SRI LANKA

Policy Title	Information and Communication Technology policy
Policy Number	06/2024
Approval Authority	The Council of the Bhiksu University Sri Lanka.
Date of Approval	11.10.2024
Next Scheduled Review	In a cycle of two years or as need arises
Review Date (s)	
Edition No.	01
Date of Effect	
Enforcement Authority	The Vice-Chancellor of the Bhiksu University Sri Lanka.
Operational Responsibility	The Director of the ICT Centre of the Bhiksu University of Sri Lanka.
Description in Brief	This policy is designed to guide the Bhiksu University of Sri Lanka (BUSL) community in the responsible use of Information and Communication Technology (ICT). It establishes a framework for managing IT systems, safeguarding information assets.

Table of Contents

1 INTRODUCTION

This Information and Communication Policy (ICT Policy) is designed to support the academic, research, and administrative functions of Bhiksu University of Sri Lanka (BUSL) by ensuring a robust, secure, and efficient ICT environment. The policy delineates the responsibilities of all users and the university in maintaining the integrity and security of the information assets of the University.

2 SCOPE

This policy governs the conduct of all Faculties, Departments, Staff, Students, and Affiliated individuals in relation to the information and communication technology resources of the Bhiksu University of Sri Lanka.

3 OBJECTIVES

3.1 Supporting Academic and Research Activities

Enhance the availability and utility of ICT resources to foster innovation and excellence in teaching, learning, and research.

3.2 Protecting Information Assets

Ensure the integrity, availability, and confidentiality of university data.

3.3 Promoting Responsible Usage

Encourage ethical and responsible use of ICT resources.

3.4 Maintaining Security and Privacy

Implement comprehensive measures to protect the university's ICT systems and the personal information of its community.

4 POLICIES AND GUIDELINES

4.1 Supporting Academic and Research Activities

4.1.1 Resource Allocation

To provide essential Information and Communication Technology (ICT) resources that underpin academic excellence and foster innovation in research and teaching at Bhiksu University of Sri Lanka.

4.1.1.1 Resources Provided:

4.1.1.1.1 **High-Speed Internet Access**

a) **Availability:** Ensure uninterrupted, high-speed internet access across all university locations, including libraries, laboratories, lecture halls, and offices.

b) **Bandwidth Management:** Regularly assess and upgrade bandwidth to meet the growing demands of academic activities and research, ensuring optimal speed and reliability.

c) **Wireless Access Points:** Expand and maintain robust wireless connectivity in all areas of the University to facilitate mobile learning and research.

4.1.1.1.2 **Specialized Software**

a) **Academic Software Licensing:** Provide licenses for software critical to academic disciplines, including statistical analysis, design, simulation, and programming tools.

b) **Research Software Support:** Offer specialized research software tailored to advanced studies and innovation, with emphasis on cutting-edge tools across various research fields.

c) **Updates and Maintenance:** Regularly update all software to ensure access to the latest features and security patches.

4.1.1.1.3 **Technical Support**

a) **Help Desk Services:** Establish a dedicated ICT help desk available to all university members, providing support for technical issues, software installation, and troubleshooting.

b) **Training and Workshops:** Offer ongoing training sessions and workshops to staff, and students to enhance their proficiency in using advanced ICT tools effectively.

c) **Maintenance and Upgrades:** Implement a proactive maintenance schedule for all ICT equipment to minimize downtime and extend the lifecycle of resources.

4.1.1.2 Implementation Strategies:

4.1.1.2.1 **Budget Allocation**

a) **Funding:** Ensure adequate annual budgeting for ICT resources, considering the need for upgrades, new technologies, and emergency responses to technological advancements.

b) **Grant Assistance:** Encourage and support departments in applying for external funding and grants that can be used to acquire or upgrade specialized software and hardware.

4.1.1.2.2 Collaboration and Partnerships

a) **Vendor Relationships:** Develop strategic partnerships with technology vendors to secure cost-effective procurement and service agreements.
b) **Inter-Institutional Agreements:** Engage in partnerships with other academic institutions for resource sharing and access to specialized tools not available within the university.

4.1.1.2.3 Monitoring and Evaluation

a) **Usage Metrics:** Regularly review the usage statistics of internet bandwidth and software licenses to adjust resources according to actual needs.
b) **Feedback Mechanism:** Implement a feedback system where students and staff can report on ICT resource issues and suggest improvements, ensuring responsiveness to the evolving academic environment.

4.1.1.2.4 Sustainability Considerations

a) **Energy Efficiency:** Prioritize the acquisition of energy-efficient technologies to reduce the environmental impact and operational costs associated with ICT resources.
b) **E-waste Management:** Develop a policy for the disposal and recycling of outdated electronic equipment in an environmentally responsible manner. All information and software must be securely wiped from IT equipment before disposal or re-use of the equipment.

4.1.1.2.5 Compliance and Security

a) **Data Security:** Ensure all systems comply with national and international data protection regulations to safeguard sensitive academic and research data.
b) **Access Controls:** Apply strict access controls to specialised software/ Servers and sensitive resources to prevent unauthorised use and ensure academic integrity.

4.2 Protecting Information Assets

Ensure the protection of the information assets of the University against unauthorised access, loss, theft, or corruption through robust data management and access control systems.

4.2.1 Data Management

4.2.1.1 Data Storage:

a) **Secure Storage Solutions:** Utilize secure servers and cloud services with strong encryption protocols for storing sensitive and confidential data.
b) **Data Segregation:** Classify data based on sensitivity and apply appropriate storage solutions to ensure that sensitive data is stored with higher security measures.

4.2.1.2 Data Transfer:

a) **Secure Transfer Methods:** Mandate the use of secure transfer protocols such as HTTPS, SFTP, and encrypted email services for transferring sensitive data.
b) **Data Transfer Agreements:** Require formal agreements for data sharing that specify the security requirements and responsibilities of both parties.

4.2.1.3 Data Backup

a) **Regular Backups:** Schedule regular backups of all critical data to multiple secure locations, ensuring redundancy.
b) **Backup Testing:** Periodically test backup systems to ensure that data restoration processes are effective and reliable.
c) **Disaster Recovery Plans:** Develop and maintain comprehensive disaster recovery plans that include procedures for restoring data in the event of data loss or system failure.

4.2.2 Access Control

4.2.2.1 Authentication and Authorization

a) **Strong Authentication:** Implement multi-factor authentication (MFA) for accessing university networks and sensitive systems.
b) **Role-Based Access Control (RBAC):** Assign access rights based on user roles and responsibilities, ensuring that individuals have access only to the resources necessary for their job functions.
c) **User Responsibilities**
    I. Care must be taken with all IT equipment to ensure its proper use and maintenance.

II. All assigned IT equipment and software remain the property of Bhiksu University of Sri Lanka. Users are obligated to safeguard and use this equipment and software only as intended by the University.

III. Direct connections of non-Bhiksu University of Sri Lanka equipment to the wired network or WLAN are prohibited unless specifically authorized and approved, as outlined in the Third-Party Access Policy.

IV. Use of personally owned information processing facilities (e.g., iPads, Smartphones) to process university information requires formal authorization and the use of authorized and secured products.

V. Removal of any IT equipment from the university premises, other than laptops, requires authorization from Information Services and relevant system owners or line managers.

VI. IT equipment must not be exposed to environmental hazards, such as extremes of temperature.

VII. Installation of software on IT equipment is prohibited without prior consultation with the ICT Centre of the University.

VIII. Modifications to IT equipment, including hardware and software configurations, are strictly forbidden.

IX. Protection measures must be in place to safeguard IT equipment against loss, theft, and unauthorized access

   a. Ensure physical security of computer equipment at all times, whether in offices or during travel.
   b. Secure equipment in the office when not in use elsewhere.
   c. Avoid leaving equipment visible in a vehicle or unattended.
   d. Use Kensington locks, where issued or available, to enhance physical security.
   e. Never leave equipment unattended, such as when traveling or in restaurants.
   f. Evaluate and implement additional security measures appropriate for the equipment's location.

X. Computer PINs, usernames, or passwords should not be stored with the equipment.

XI. Important files should not be stored solely on computers to prevent complete data loss in case of equipment failure or theft.

XII. Any lost or stolen equipment must be reported immediately to the ICT Centre of the University.

4.2.2.2 User Account Management:

a) **Account Lifecycle Management:** Establish procedures for creating, modifying, and deactivating user accounts aligned with personnel changes such as new hires, role changes, and departures.
b) **Regular Access Reviews:** Conduct periodic reviews of access rights to ensure that they remain appropriate and that there are no orphaned accounts or excessive privileges.

4.2.2.3 Password

a) All workstations must be protected with a password.
b) Authorised users are responsible for the security of their passwords and user accounts. Passwords must be kept secure and never shared with anyone else.
c) Passwords must be at least 12 characters long and include alpha, numeric and at least one other character. Their structure must make them hard to guess. Guidance on creating passwords is available on the University Intranet.
d) Passwords should never be displayed on screens.
e) If at any time a user believes their password has been compromised, they must immediately change it or request that it is changed.
f) Should a user request a password change on their behalf, proof of identity will be required as for account/password creation.
g) Passwords should never be "remembered" on the computer but entered by the user on all occasions.

4.2.2.4 Monitoring and Logging:

a) **Audit Trails:** Maintain logs of access and activities on sensitive systems and use automated tools to analyze logs for unusual activities that might indicate a security breach.
b) **Anomaly Detection:** Utilize advanced anomaly detection systems to identify and respond to unauthorized access attempts in real time.

4.2.2.5 Physical Security:

a) **Secure Facilities:** Ensure that physical access to critical infrastructure, such as data centers and server rooms, is strictly controlled and monitored with access logs, surveillance cameras, and entry authentication systems.
b) **Environmental Controls:** Install environmental controls to protect IT assets from physical threats like fire, water damage, and extreme temperatures.

4.2.2.6 Compliance and Training

a) **Legal Compliance:** Regularly update access control and data management policies to comply with relevant data protection laws and regulations.
b) **Security Awareness Training:** Provide ongoing security training to all university personnel to raise awareness about the importance of data security and the specific practices required to maintain it.

4.3 E-Mail Use

E-mail enhances communication but poses risks like malicious attacks and privacy breaches. All e-mail systems accessed on university or personal devices are considered university property. Usage is monitored and inappropriate use may result in disciplinary action.

4.3.1 Usage and Guidelines

4.3.1.1 Dos:

- Observe all applicable laws and copyright rules.
- Verify recipients and message necessity before sending.
- Use shared directories for large files to save bandwidth.
- Be cautious with e-mails from unknown sources; verify attachments for malware.
- Ensure e-mail content is objective and necessary.

4.3.1.2 Don'ts:

- Use e-mail for personal gain or unauthorized activities.
- Send spam, chain letters, or offensive content.

- Store or transmit sensitive information without proper security measures.
- Engage in or respond to phishing attempts.

4.3.1.3 Procedures:

- Report misdirected or suspicious e-mails to a Head of the Department (HoD).
- Confirm the authenticity of requests for sensitive information verbally and through managerial approval.

4.3.1.4 Security Measures:

- Use strong encryption for transmitting sensitive data.

4.4 Promoting Responsible Usage

Encourage the responsible and ethical use of the ICT resources of the University, promoting an environment that supports academic integrity, respects privacy, and maintains the security of digital information.

4.4.1 Usage Policy: Guidelines for Lawful and Ethical Use

4.4.1.1 Acceptable Use Guidelines

a) **Purpose of Use:** ICT resources must be used primarily for academic, research, and administrative purposes. Personal use is permitted where it does not interfere with these primary purposes and complies with all university policies.
b) **Respect for the University Values:** All digital activities should align with core values of the University, including respect for diversity, integrity, and the pursuit of knowledge.

4.4.1.2 Ethical Behavior:

a) **Intellectual Property:** Respect copyrights, trademarks, and all forms of intellectual property rights. Unauthorized copying, distribution, or modification of software, data, or digital content is prohibited.
b) **Confidentiality:** Maintain the confidentiality of proprietary or sensitive information. Do not disclose personal or university data without proper authorization.

4.4.1.3 Legal Compliance:

a) **Regulatory Adherence:** Comply with all local, national, and international laws regarding online conduct and acceptable content.
b) **Reporting Obligations:** Immediately report any security breaches or misuse of ICT resources to the appropriate university authorities.

4.4.2 Prohibited Activities

4.4.2.1 Unauthorized Commercial Activities:

a) **No Commercial Gain:** Do not use university ICT resources for personal business, commercial gains, or any for-profit activities without explicit authorization from the university.
b) **Advertising and Promotion:** Prohibit the use of ICT resources for distributing advertisements or promotional material unless part of an approved university activity.

4.4.2.2 Harassment and Offensive Behavior:

a) **Zero Tolerance for Harassment:** The University strictly prohibits the use of ICT resources to engage in behavior that could be considered harassing, bullying, or discriminatory.
b) **Offensive Content:** Prohibit the creation, display, or circulation of content that is offensive, obscene, or otherwise harmful. This includes, but is not limited to, sexually explicit material, hate speech, and violent imagery.

4.4.2.3 Security Risks:

a) **Hacking and Unauthorized Access:** Forbid any attempt to gain unauthorized access to any computer systems or networks. This includes the distribution of malicious software or the exploitation of security vulnerabilities.
b) **Resource Misuse:** Prohibit the use of ICT resources in a way that could damage, disable, overburden, or impair any university networks or interfere with any other party's use and enjoyment of university ICT resources.

4.4.3 Enforcement and Compliance

4.4.3.1 Monitoring and Audits:

a) **Activity Monitoring:** The University reserves the right to monitor ICT usage to ensure compliance with policies. Users should have no expectation of privacy when using university resources.
b) **Regular Audits:** Conduct periodic audits of ICT resource usage to detect and address policy violations.

4.4.3.2 Disciplinary Actions:

a) **Consequences of Violations:** Violations of the usage policy may result in disciplinary actions, which could include suspension of access to ICT resources, formal reprimands, and in severe cases, termination of employment or expulsion from the University.
b) **Appeal Process:** Provide a clear process for users to appeal against decisions made regarding alleged misuse of ICT resources.

4.5 Maintaining Security and Privacy

To safeguard the ICT systems of the University from cyber threats and ensure the privacy of all community members through stringent security measures and privacy protocols.

4.5.1 Security Measures

4.5.1.1 Antivirus and Anti-malware Solutions:

a) **Implementation:** Install and maintain reputable antivirus and anti-malware software on all university-owned devices and systems.
b) **Regular Updates:** Ensure that antivirus and anti-malware definitions are updated regularly to respond to new threats as they emerge.
c) **System Scans:** Schedule regular scans to detect and remove malicious software from devices and network systems.

4.5.1.2 Firewalls

a) **Network Firewalls:** Deploy robust firewall solutions at network perimeters to monitor and control incoming and outgoing network traffic based on predetermined security rules.
b) **Host-Based Firewalls:** Install and configure firewalls on individual devices to provide an additional layer of protection.

4.5.1.3 Intrusion Detection Systems (IDS)

a) **Deployment:** Implement network-based and host-based IDS to continuously monitor network and system activities for malicious activities or policy violations.
b) **Real-Time Alerts:** Configure IDS to send real-time alerts to the IT security team for immediate action on detected threats.

4.5.1.4 Data Encryption:

a) **At Rest and In Transit:** Encrypt sensitive data both at rest and in transit to protect it from unauthorized access.
b) **Encryption Standards:** Utilize strong encryption standards such as AES-256 for data storage and transport layer security (TLS) for data transmission.

4.5.1.5 Patch Management:

a) **Regular Updates:** Establish a routine process for applying security patches and updates to all software and operating systems to close vulnerabilities.
b) **Vulnerability Assessments:** Regularly perform vulnerability assessments and remediate identified weaknesses promptly.

4.5.2 Privacy Protocols

4.5.2.1 Data/ Information Classification and Handling

a) **Classification:** Classify data/ Information based on sensitivity and apply appropriate handling and storage measures to each classification level such as;
    I. **Public** - non-sensitive information, the unauthorised disclosure, modification or loss of which would cause no damage to the University

II. **Internal** - information not intended for a public audience, but the unauthorised disclosure, modification or loss of which would have a minimal impact on the interests of the University

III. **Restricted** - private information, the unauthorised disclosure, modification or loss of which would be detrimental to the interests of the University

IV. **Confidential** - Sensitive information, the unauthorised disclosure, modification or loss of which would cause significant harm to the interests of the University

b) **Access Policies:** Ensure that access to sensitive information is strictly controlled and limited to authorized personnel only.

4.5.2.2 Data Control

a) The Bhiksu University of Sri Lanka information classified as Confidential may only be transmitted electronically if approved by the information owner and when it is secured appropriately according to all applicable policies and standards based on its level of classification.

b) Users may not copy Bhiksu University of Sri Lanka information classified as Confidential to personal storage devices (e.g. any device not owned or managed by the Bhiksu University of Sri Lanka), including but not limited to USB, external drives, smartphones and tablets.

c) Users may not synchronise or share Bhiksu University of Sri Lanka Confidential information using internet enabled commercial services with file sharing capabilities (e.g. DropBox,). Only services which are managed and operated by the Bhiksu University of Sri Lanka may be used for this purpose.

4.5.2.3 Privacy Impact Assessments:

a) **Assessment Process:** Conduct privacy impact assessments for new projects or changes to existing systems that handle personal data to identify potential privacy issues.

b) **Mitigation Strategies:** Implement mitigation strategies to address risks identified during the assessments.

4.5.2.4 Compliance with Privacy Laws

a) **Legal Framework:** Adhere to applicable local, national, and international privacy laws and regulations governing the protection of personal information.
b) **Policy Updates:** Regularly review and update privacy policies to ensure ongoing compliance with legislative changes.

4.5.2.5 Training and Awareness

a) **Regular Training:** Provide mandatory privacy training to all employees and students to enhance their understanding of privacy obligations and proper handling of personal data.
b) **Awareness Programmes:** Conduct awareness Programmes to keep the university community informed about privacy rights and responsibilities.

4.5.2.6 Incident Response and Notification

a) **Incident Response Plan:** Develop and maintain an incident response plan to address data breaches or privacy violations effectively.
b) **Breach Notification:** Establish protocols for timely notification to affected individuals and regulatory bodies in the event of a significant privacy breach.

5 COMPLIANCE AND ENFORCEMENT

To ensure strict adherence to the ICT policies through systematic monitoring and enforcement procedures that uphold the standards and security measures set by Bhiksu University of Sri Lanka.

5.1 Monitoring

5.1.1 ICT Resource Monitoring:

a) **Purpose:** Monitor the use of all ICT resources to detect and prevent policy violations, potential security threats, and to ensure optimal performance.
b) **Scope:** Include monitoring of network traffic, system usage, application activity, and access logs.

c) **Transparency:** Clearly communicate to all users that their use of the University ICT resources is subject to monitoring. This includes ensuring that all users are aware of the monitoring activities through user agreements and notification upon login.

5.1.2 Audit and Review:

a) **Regular Audits:** Conduct regular audits of ICT systems to ensure compliance with internal policies and external regulatory requirements.
b) **Audit Reports:** Generate audit reports detailing compliance status, issues found, and recommendations for improvement.
c) **Review Process:** Periodically review the monitoring and audit procedures to enhance their effectiveness and to adapt to new technological and regulatory developments.

5.2 Penalties for Non-compliance

5.2.1 Graduated Penalty System:

a) **Minor Violations:** Address minor infractions, such as unauthorized minor use of resources, with warnings and a review of policy requirements.
b) **Serious Violations:** Respond to more serious infractions, such as unauthorized access to sensitive data or malicious activities, with stricter penalties including suspension of ICT resource access, formal reprimand, or mandatory training on compliance and security practices.

5.2.2 Severe Non-compliance:

a) **Suspension or Termination:** For severe violations, particularly those involving illegal activities or causing significant harm to the ICT systems of the University, suspend or terminate access to ICT resources. Additionally, take disciplinary actions which could include expulsion or termination of employment, depending on the nature of the violation.
b) **Legal Action:** Pursue legal action against individuals who commit unlawful acts using the ICT resources of the University. This includes cooperation with law enforcement agencies and compliance with court orders.

5.2.3 Reporting Mechanism:

5.2.3.1 Incident Reporting

Establish a clear mechanism for reporting violations of the ICT policy, which can be accessed by all members of the University.

5.2.3.2 Anonymous Reporting

Include provisions for anonymous reporting to encourage the reporting of violations without fear of reprisal.

5.2.3.3 Reporting of Security Incidents and Personal Data Breaches

At the Bhiksu University of Sri Lanka, all security incidents, including personal data breaches, must be logged and managed. While all personal data breaches are considered security incidents, not all security incidents qualify as personal data breaches. Security incidents may require reporting to the ICT Centre within 72 hours if they involve a personal data breach. Report any suspected or known security incidents or breaches directly to the ICT Centre immediately.

5.2.3.3.1 **Examples of Security Incidents:**

- Loss or theft of equipment or sensitive data.
- Physical damage to IT equipment.
- Unauthorized access to user profiles or sensitive information.
- Sharing passwords without authorization.
- Misuse of email or the internet, such as harassment or accessing prohibited content.
- Unauthorized copying of data or damage to property impacting security.
- Unauthorized access to premises or theft of IT equipment.

5.2.3.3.2 **Handling Incidents:**

- Do not attempt to resolve security incidents beyond basic corrective steps (e.g., recalling a misdirected email).
- Avoid actions that could compromise data integrity or evidence.

- Report non-IT related personal data breaches, like misplaced paperwork, to the Information Centre for further action.

5.2.3.3.3 **Guidance:**

- Consult a Line Manager if unsure about the appropriate actions to take following a security incident.

5.2.4 Handling of Violations:

a) **Investigation Procedures:** Develop standardized procedures for investigating reported or detected violations of the ICT policy.
b) **Fairness and Impartiality:** Ensure that all investigations are conducted fairly and impartially, with an opportunity for the accused parties to respond to allegations.

5.2.5 Documentation and Records:

a) **Record-Keeping:** Maintain detailed records of all violations and the subsequent actions taken. This includes documentation of investigations, disciplinary actions, and communications with the involved parties.
b) **Confidentiality:** Handle all records related to compliance and enforcement confidentially, in accordance with applicable privacy laws and policies of the University.

6 REVIEW AND AMENDMENTS

To maintain a dynamic and responsive ICT Policy that adapts to new security threats, technological advancements, and changes in legal and regulatory frameworks.

6.1 Policy Review

6.1.1 Annual Reviews:

a) **Scheduled Assessments:** Conduct a formal review of the ICT Policy on an annual basis to ensure it aligns with the latest ICT practices and complies with current laws and regulations.

b) **Involvement:** Involve key stakeholders in the review process, including IT management, cybersecurity teams, legal advisors, and representative users from, staff, and student bodies.

6.1.2 Ad-Hoc Reviews:

a) **Trigger Events:** In addition to annual reviews, undertake ad-hoc policy evaluations in response to significant incidents, such as data breaches, major IT infrastructure changes, or new legislative requirements.
b) **Feedback Mechanism:** Implement a mechanism for the community of the University to suggest changes or report issues with the current policy, facilitating ongoing improvements and adaptation.

6.2 Policy Amendments

6.2.1 Amendment Proposals:

a) **Proposal Submissions:** Allow for the submission of amendment proposals by stakeholders through a formal process. Proposals should detail the reasons for changes, the expected benefits, and any potential impacts on current systems and practices.
b) **Review Committee:** Establish a review committee to evaluate amendment proposals based on their necessity, feasibility, and alignment with university objectives and compliance requirements.

6.2.2 Approval and Implementation:

a) **Decision Making:** The review committee should recommend approval, modification, or rejection of amendment proposals. Final approval will be made by a designated authority such as a governance board of the University.
b) **Implementation Plan:** For approved amendments, develop an implementation plan that includes timelines, resource allocations, and responsibilities. Communicate the changes to all affected parties and provide training if necessary.

6.2.3 Documentation and Communication:

a) **Documentation Updates:** Upon approval of any amendments, update all documentation related to the ICT Policy to reflect the changes.
b) **Broad Communication:** Distribute the revised policy across the University through multiple channels to ensure that all users are aware of the new rules and their implications.

6.2.4 Monitoring the Impact of Changes:

a) **Impact Assessment:** Monitor the implementation of changes to evaluate their impact on ICT operations and security. Adjust the implementation plan based on observed outcomes and feedback from users.
b) **Continuous Improvement:** Use insights gained from monitoring and feedback to make further refinements to the policy, fostering a culture of continuous improvement in managing ICT resources.

7 ACKNOWLEDGMENT

To ensure that all users of the ICT resources of the University are fully informed about the policies governing their use and agree to adhere to these guidelines as a condition of their access.

7.1 Agreement Formulation:

a) **Content:** Develop a user agreement form that clearly states the responsibilities and obligations of users regarding the use of ICT resources. This agreement should reference the ICT policy document and summarize key points, such as acceptable use, security practices, and penalties for non-compliance.
b) **Accessibility:** Ensure that the user agreement is accessible in both digital and physical formats and is easy to understand, avoiding overly technical language where possible.

7.2 Mandatory Acknowledgment:

a) **At Onboarding:** Require all new users (including faculty, staff, and students) to read and sign the user agreement as part of their orientation process before they are granted access to ICT resources.
b) **Periodic Re-acknowledgment:** Mandate that all users re-acknowledge the agreement on a periodic basis, such as annually, to ensure ongoing awareness and compliance.

7.3 Digital Signature:

a) **Implementation:** Utilize a digital signature platform to facilitate the acknowledgment process, allowing users to sign the agreement electronically. This process should be secure and verify the identity of each user.

b) **Record Keeping:** Maintain electronic records of all signed agreements, ensuring that they are stored securely and can be accessed by authorized personnel when needed for audits or disciplinary actions.

7.4 Training and Education:

a) **Awareness Programmes:** Accompany the user agreement with educational Programmes that provide users with understanding of the policy details. This can include online training modules, workshops, and informational sessions.

b) **Resources Availability:** Make detailed ICT policy documents readily available to all users through the university's intranet or a designated online portal. Encourage users to consult these resources regularly to stay informed about any changes or updates.

7.5 Condition of Access:

a) **Access Restriction:** Clearly state that access to the ICT resources of the University is conditional upon the signing of the user agreement. Users who do not agree to the terms should not be granted access.

b) **Compliance Enforcement:** Use the signed agreement as a binding document that can be referenced in disciplinary actions if a user fails to comply with the ICT policies.

7.6 Handling Non-compliance:

a) **Procedures for Non-signature:** Establish procedures for handling cases where users refuse to sign the agreement, including providing additional counselling to explain the importance and implications of the agreement.

b) **Consequences:** Outline the consequences of failing to sign the agreement, such as restricted access to ICT resources, which could affect the user's ability to perform academic or administrative functions.

8 TERMINOLOGICAL CLARIFICATIONS (DEFINITIONS)

Information and Communication	Refers to the infrastructure and components that

Technology (ICT)	enable modern computing, including all forms of computer and communications equipment, software, and network systems used to create, store, transmit, and analyze digital information.
Bhiksu University of Sri Lanka (BUSL)/ The University	This term as referred to within the context of this Social Media Policy and all associated digital assets, denotes the Bhiksu University of Sri Lanka. This designation is based on the legislative provisions outlined in the Buddhasravaka Bhiksu University Act, No. 26 of 1996, and further amended by the Buddhasravaka Bhiksu University (Amendment) Act, No. 15 of 2012, whereby the original name "Buddhasravaka Bhiksu University" has been officially replaced with "Bhiksu University of Sri Lanka."
ICT Resources	Collective term for all technology systems, hardware, software, networks, data, and communication facilities managed by the university.
User	Any individual, including staff, students, faculty, and affiliates, who accesses or uses the ICT resources provided by BUSL.
Security Incident	Any event that results in unauthorized access, use, disclosure, disruption, modification, or destruction of information or ICT systems.
Personal Data Breach	A security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data processed by the university.
Multi-Factor Authentication (MFA)	A security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.
Role-Based Access Control (RBAC)	A method of restricting network access based on the

	roles of individual users within an enterprise and ensuring that only authorized users have access to certain data or resources.
Intrusion Detection Systems (IDS)	Devices or software applications that monitor networks or systems for malicious activity or policy violations.
Data Encryption	The method of converting plaintext data into a secret code that hides the data's true meaning to prevent unauthorized access.
Patch Management	The process of distributing and applying updates to software to correct security vulnerabilities and improve functionality.
Compliance	Adherence to laws, regulations, guidelines, and specifications relevant to the university's operations.
Audit	A systematic review of records and activities to ensure compliance with established policies, procedures, and operational processes.
Data Privacy	Involves the proper handling, processing, storage, and usage of personal information in accordance with protection laws and regulations.
Digital Signature	A mathematical scheme for demonstrating the authenticity of digital messages or documents, securing processes such as software distribution, financial transactions, and contract management.
Head of Department (HoD)	The individual in charge of an academic or administrative department within BUSL, responsible for enforcing policy within their domain.

-END-