Sabaragamuwa University of Sri Lanka

Policy Title – **Policy on Information and Communication Technology (ICT) of Sabaragamuwa University of Sri Lanka**

Policy Number – Policy / SUSL / Gov & Mgmt / 04

Effective Date – 29.11.2021

Revised Dates – NA

Approving Authority – The Council, Sabaragamuwa University of Sri Lanka

Administrative Responsibility –Senate, Council

Content

1 Information and Communication Technology Policy

1.1 Purpose

The Sabaragamuwa University of Sri Lanka of Sri Lanka (SUSL) has provided Information Communication Technology (ICT) facilities for the activities related to the academic, research and administrative operations and activities of the academic and non-academic staff, students, alumni and government because the university has identified that providing access to the ICT related activities is giving the huge opportunities and more information can be collected for the educational purposes. As more information is created, used, and shared in digital form by students, faculty, and staff, an increased effort must be made to acquire IT resources of the highest standards, as well as to protect all the ICT facilities that support such initiatives. So this policy is providing two purposes. Those are,

1. Increasing data protection and ICT facilities by ensuring usability, reliability, and availability of those facilities.

2. Aligning the University’s ICT infrastructure, architecture, and operational activities with the industry best practices.

This policy applies to all members of the university community and those who use university ICT facilities. When decisions are made regarding the acquisition and management of ICT infrastructure, architecture, and operational activities, the decision-maker should consult this policy for guidance.

1.2 Scope

This policy applies to all internal and external users of the SUSL ICT facilities.

Users

This policy applies to everyone who accesses the SUSL ICT facilities, whether affiliated with the university or not, whether on campus or from remote locations, including but not limited to students, faculty, staff, consultants, temporary employees, guests, volunteers, and contractors. More specifically for:

a. Internal students with a valid registration.
b. Staff in current employment with the SUSL, either permanent, temporary or contract.
c. Personnel of the SUSL departments, divisions, projects, etc., with a valid authorization for the use of ICT facilities given by the head of the relevant unit.
d. External users with a valid authorization for ICT facilities use are given either by the Head of the relevant unit or CCS.

ICT facilities

University-owned personal computers, servers, computer peripherals, storage, services, software, wired and wireless networks, internet connections, transmission lines, and exchanges are included in ICT facilities. As well information recorded on all types of electronic media, computer hardware and software, documentaries or paper (file), computer networks, telephone systems, personal computers, servers, computer peripherals, storage, wired and wireless networks, and other devices not owned by the university, but intentionally connected to the university-owned ICT facilities while so connected.

If any user is going to access or use university ICT facilities means that the user has agreed to comply with this policy.

1.3 Policies and Laws

The following policies are using to build up this policy

1. Acceptable Use Policy
2. Administrator Access Policy
3. Usage Policy of Computer Laboratories
4. Policy of Electronic Communication
5. Policy of Incident Response on Information Security
6. Network Protection Policy
7. Password Policy
8. Web Privacy Statement Policy
9. Social Media Policy
10. E-Learning Policy
11. Hardware and Software Disposal Policy/IT Assets Disposal Policy
12. Website Use and Update Policy

All the policies mentioned above are working together to build up the whole policy. Therefore, any specific case should be handled according to the combinations of these policies and all other applicable approved policies by the university community. As well whole university community should be aware of this policy and national laws which may be breached by them and they should take responsibility if they have done illegal activities and penalties by using the university ICT facilities. Some of the legislated acts of parliament in this respect are:

1. Computer Crimes Act No. 24 of 2007 of Sri Lanka
2. Electronic Transaction Act No. 19 of 2006 of Sri Lanka
3. Electronic Transactions (Amendment) Act, No. 25 of 2017
4. Intellectual Property Act No. 36 of 2003 of Sri Lanka

1.4 Contact Information

Users who require clarifications or comment on this policy or forthcoming policies, or who wish to report a policy violation should contact,

Director: Centre for Computer Studies
E-mail: director@ccs.sab.ac.lk

1.5 Abbreviations

AUP	-	Acceptable Use Policy
CCS	-	Centre for Computer Studies
DHCP	-	Dynamic Host Configuration Protocol
EVLE	-	Examination Virtual Learning Environment
ICT	-	Information Communication Technology
LEARN	-	Lanka Education and Research Network
OS	-	Operating Systems
SUSL	-	Sabaragamuwa University of Sri Lanka of Sri Lanka
UPS	-	Uninterrupted Power Supply
URL	-	Uniform Resource Locator
UTP	-	Unshielded Twisted Pair
VLE	-	Virtual Learning Environment

2 SUSL.ICT.2021.1 - Acceptable Use Policy

ICT Policy Document **Centre for Computer Studies** **Sabaragamuwa University of Sri Lanka of Sri Lanka**	**Published Date:**	**Policy No:** **SUSL.ICT.2021.1**
Policy: Acceptable Use Policy	**Approval Date:**	**Page No:**

Objectives: The aim of this Acceptable Use Policy (AUP) for SUSL ICT facilities is to protect the 'SUSL's vital interests while not unduly restricting the use of ICT facilities and services that have been developed for the benefit of students, employees, and the SUSL as a whole.	
Responsible Official	
Responsible Office	
Signature	

2.1 Executive Summary

The hardware and software which were established in the Local Area Network of the Sabaragamuwa University of Sri Lanka of Sri Lanka are vital to its operations. Inappropriate use of the network and its components can detrimentally accomplishing the institution's mission. Every user of the network has a responsibility to utilize these shared resources in an appropriate manner. The Acceptable Use Policy addresses this responsibility.

2.2 Scope:

The Acceptable Use Policy applies to all users mentioned below who are utilizing the ICT facilities of the Sabaragamuwa University of Sri Lanka of Sri Lanka.

2.2.1 Users

This policy extends to everyone who uses the SUSL ICT services, whether or not they are associated with the university, whether on campus or off, and whether they are students, permanent employees, consultants, temporary employees, visitors, volunteers, or contractors. More precisely for:

1. Internal students with a currently valid registration.
2. Staff in current employment with the SUSL, either permanent, temporary or contract.
3. Personnel of the SUSL departments, divisions, projects, etc., with a valid authorization for the use of ICT facilities given by the head of the relevant unit.
4. External users with a currently valid authorization for ICT facilities use either by the

Head of the relevant department/division or Center for Computer Studies (CCS).

2.2.2 ICT facilities

Personal computers, servers, computer peripherals, storage, power generators, utilities, applications, wired and wireless networks, Internet links, transmission lines, and exchanges are all examples of items covered by this policy. The information recorded on all forms of electronic media, computer hardware and software, paper (files), computer networks, and telephone systems are examples of ICT facilities operated by the university and those used by the university under license or contract. Personal computers, servers, computer peripherals, storage, wired and wireless networks, and other devices not operated by the university but deliberately linked to the University-owned ICT facilities while so connected are all examples of ICT facilities.

Above users are given access to the SUSL ICT facilities for the purpose of:

1. Conducting and participating in academic coursework and research.
2. Performing and using academic and non-academic administrative services.
3. Conducting and participating in University-approved student and staff welfare services.
4. Conducting and participating in University-approved projects.
5. Utilizing and accessing the teaching & learning and information services provided by the library network of the university.

For reasonable use, the students and staff are not charged a fee, and the SUSL bears the cost of providing access to the SUSL computing, storage, and network (including internet) resources.

2.2.3 ICT Facilities Covered Under AUP

For the understanding and the application of this AUP, smart devices such as mobile phones, tablets, and wearable are considered as computers.

This AUP is applicable to the following equipment and services:

1. To all computers (university-owned or not) when they are on SUSL property, including campuses, project buildings, and hostels.

2. To all computers, computer peripherals, detachable storage devices, and network equipment (university-owned or not) connected to the SUSL wired and wireless networks.

3. To all university-owned computers, computer peripherals, utilities, and applications that are used off-campus.

4. To all information and communication technology (ICT) facilities in lecture theaters, labs, and libraries and offices of the university.

5. To all internet accesses, remote access, and electronic messaging services (e.g., e-mail, instant messaging, VoIP, library bulk e-mails and newsgroups) made possible by SUSL ICT facilities.

6. To all user accounts on SUSL's systems.

7. To all forms of data processed on the SUSL's information technology infrastructure.

8. To all proprietary and open-source software for which the SUSL holds licenses, as well as software developed customized for the use of the SUSL.

2.3 Policy:

Above mentioned users are expected to follow the rules and regulations of the policy for authorized access to network information and university resources.

2.3.1 Permitted Activities Covered under AUP

The SUSL ICT facilities are expected to be used for the following activities:

1. Access to authorized academic course materials, research resources, library services and online activities hosted within the SUSL ICT facilities.
2. Access to materials hosted outside the SUSL ICT facilities for study, research, and academic or non-academic administrative purposes.
3. Access to software and equipment used in academic study, research, library services and academic or non-academic administrative work hosted within the SUSL ICT facilities.
4. Access to software and equipment hosted outside the SUSL ICT facilities for study, research, and academic or non-academic administrative purposes.

5. For organizing and managing academic, research, administrative work, library outreach and university authorized extra-curricular activities.

6. For the development of software for academic, research, and administrative purposes.

7. For limited recreational purposes that are in strict conformity with this AUP including restrictions on resource usage, time of use, intellectual property rights, applicable civil and criminal laws.

2.3.2 Prohibited Activities Covered under AUP

It is strictly forbidden for users of SUSL ICT facilities to misuse the equipment, services, or facilities. Some examples of forbidden practices are mentioned below

1. Unauthorized access SUSL ICT facilities from an account other than their own.
2. Unauthorized access to any equipment, data, and services on SUSL ICT facilities.
3. Installing unauthorized programs (proprietary or open-source) on SUSL ICT facilities.
4. Unauthorized removing, changing computer hardware and other equipment.
5. Conducting unauthorized commercial activities on SUSL ICT facilities without a prior authorization from the relevant SUSL authorities.
6. Using ICT facilities to sell, purchase, or broker in assignments, to solicit or offer to write assignments for others.
7. Using electronic messaging services form knowingly originating or retransmitting messages that are defamatory; aggressive or rude to other users; threatening or harassing; containing political and religious views, containing pornographic or sexually explicit content; bulk, unsolicited, and spamming; chain e-mail; seeking to impersonate another person (spoofing); containing malware such as viruses, worms, phishing attacks and Trojans.
8. Misuse or unauthorized access, collection, storing, and dissemination of sensitive of information such as demographic information, personal health records, personal diaries, calendar notes, details in personal user accounts, mobile numbers and official e-mail address provided by the university or collected by any means including questionnaires, intellectual property, proprietary material, course notes and material, agreements in the form of MoUs and NDAs, internal memos, and data.
9. Using peer-to-peer services to access or share copyrighted material, enable anonymous access to third-parties via proxy and VPN (Virtual Private Network) services, crypto currencies.

10. Accessing pornographic materials using SUSL ICT facilities. The creation, storage, or distribution of pornographic materials is also strictly prohibited.
11. Using SUSL ICT facilities in a manner that is inequitable or disruptive to other users.

Network users are expected to treat all network hardware facilities and infrastructures with proper care and are expected to utilize all network resources in ways that respect the other network users. The following activities constitute violations of this policy:

- Damaging hardware of the University Local Area Network and it's all branches.
- Introducing viruses to any standalone machine or to the University Local Area Network.
- Deliberately slowing a system using any kind of method.
- Attempting to crash a system partially or whole system.

Discriminatory, demeaning, or abusive behavior may be subject to the 'university's Policy Statement on Harassment as described in the Student Conduct Policies on Respect for Self, Others, and the Community, Respect for Property, Personal Responsibility, or Harassment as described in the Circulars issued by the University Grant Commission. Network users are expected to use systems for authorized purposes only. Violations include activities such as: advertising for a commercial organization, running a business, activities that violate public law.

2.3.3 Responsibility of users

To ensure equal and equitable access to the services, all users of the SUSL ICT facilities must work together with other users, system administrators, and SUSL authorities. Users of ICT facilities must be mindful of the terms on which access is granted, as well as the practices that are allowed and prohibited.

The SUSL ICT facilities are accessed by a computer account that is defined by a username and protected by a password. As a result, it is imperative that:

1. Passwords must not be shared with others.
2. Users must not knowingly participate in any action with the intent of obtaining other 'users' passwords.

3. If a password breach is suspected, a user must update his or her password immediately and notify the appropriate systems administrator.

4. Users must pick and maintain a safe password and log-off after using ICT services according to the guidance issued by relevant systems administrators and the University User Accounts and Password policy.

The SUSL disclaims all liability for the following:

1. Direct or indirect losses or damages resulting from the use of SUSL ICT facilities for academic, non-academic, or personal purposes.

2. Data loss or disruption of files and resources as a result of the SUSL's efforts to preserve, secure, and upgrade ICT facilities.

Unauthorized usage of ICT services by a customer is a violation of this AUP which can result in disciplinary action. Individual users can face civil and criminal legal action if they use ICT facilities in an illegal manner. Any user who uses SUSL ICT services for illegal purposes will not be defended or supported by the SUSL.

2.4 Privacy and Laws

The SUSL reserves the right to inspect and track e-mail, websites (both official and personal), server and firewall logs, electronic files and data, software, computers, or any other electronic device that is:

1. Both wired and wireless access to the SUSL network.
2. Operated within the SUSL premises, either permanently or temporarily, regardless of equipment ownership.

Following high-level, SUSL-wide monitoring is in place on a 24x7 basis:

1. Firewall logs for initiating and accepting network connections, as well as attempts to access/use blocked services and ports.
2. Proxy logs for initiating connections to URLs.
3. Wireless access log.
4. Accounts logs such as e-mail and LMS/VLE/EVLE.

5. Server logs.

If the SUSL decides that there is a cause, it will perform these inspections and monitoring activities. There are a variety of explanations for this, including but not limited to:

1. Suspected or reported breaches of this AUP.
2. Suspected or reported breaches of any rules, regulations, or policies of the SUSL.
3. Suspected or reported breaches of the Law.

Users should be mindful of actions that can violate national laws, resulting in civil or criminal court proceedings and penalties for which they will be held legally liable. In this regard, some of the legislative acts of parliament include:

1. Computer Crimes Act No. 24 of 2007 of Sri Lanka
2. Electronic Transaction Act No. 19 of 2006 of Sri Lanka
3. Electronic Transactions (Amendment) Act, No. 25 of 2017
4. Intellectual Property Act No. 36 of 2003 of Sri Lanka

Violations of the AUP are subject to disciplinary action. In the following conditions, the SUSL reserves the right to revoke any 'user's permission to use SUSL ICT facilities:

- Any clause of this AUP is violated by the consumer.
- The 'user's use of ICT facilities puts those facilities at risk.
- The 'user's use of ICT facilities poses a security or other threat to other users, the SUSL the general public, or national security. The user violating privacy and personal rights of others.

Additionally, the SUSL may take appropriate disciplinary, administrative, and legal action under the relevant rules and regulations against the AUP violators.

2.5 Definitions:

The Local Area Network of Sabaragamuwa University of Sri Lanka of Sri Lanka is the group of stations (computers, IP phones, printers, or other devices) owned or operated by the university connected by communications facilities owned or operated by the university for exchanging information. The connection can be permanent, via cable, or temporary, through telephone or other communications links. The transmission medium can be physical (e.g., fiber optic cable) or wireless (e.g. satellite, Wi-Fi).

3 SUSL.ICT.2021.2 - Administrator Access Policy

ICT Policy Document **Centre for Computer Studies** **Sabaragamuwa University of Sri Lanka of Sri Lanka**	**Published Date:**	**Policy No:** **SUSL.ICT.2021.2**
Policy: Administrator Access Policy	**Approval Date:**	**Page No:**
Objectives: The objective of this policy is to give a clear idea on the appropriate use of Administrator Access to SUSL ICT facilities and to aid in the interpretation of requirements set in the University ICT Policy.		
Responsible Official		
Responsible Office		
Signature		

3.1 Executive Summary:

This document defines policy of the university regarding local administrator rights to Sabaragamuwa University of Sri Lanka-owned workstations. The university is committed to providing members of the University community with reliable technology in stable operating conditions while appropriately addressing the university needs and maintaining University system integrity and data security.

3.2 Scope:

The Administrator Access Policy applies to all University system and application administrators and any other personnel who are provided with “Administrator” access on the university owned computers or workstations.

3.3 Policy:

Generally, all the Faculty/Staff/Center/Unit members are assigned normal access level rights on their individual workstations. If a faculty member wants to use Administrator level access, exceptions may be granted to Faculty/Staff/Center/Unit members who require Administrator level access to perform job-related tasks. Individuals may request administrator-level access through the CCS Helpdesk (helpdesk@ccs.sab.ac.lk) and sign the Request for Administrator Access document (provided by CCS), acknowledging that they have read the Use of the University Computing Network Policy and Administrator Access Policy. The use of these rights and the level of access to the workstation are to be in accordance with the "Use of Sabaragamuwa University of Sri Lanka Local Area Network" policy.

3.4 Guidelines:

- University workstations are university property and are intended for university activities.
- Individuals should only install software related to university activities.
- Individuals should not install software that may lead to damage files and expose the university Local Area Network to virus attacks and malicious coding.
- Individuals should refrain from installing software which may monopolize local processor power, resulting in noticeable system slowdown or degradation of performance.
- Individuals should not install applications that may establish network share protocols which result in an increase in bandwidth utilization as this may cause network congestion and degradation of network performance across wide areas of the campus.
- Individuals should not download or install applications (software) that are illegal or not licensed on university-owned equipment.
- Individuals, who download or install applications (software) other than those included in the standard configuration for all the university computers, are responsible for retaining documentation of appropriate licenses.

3.5 Support:

- Non-standard software will be removed as part of a normal repair process if necessary, to restore system functionality.
- In the event of computer or network performance issues associated with a computer enabled with administrator-level access, CCS will only restore the computer to the standard configuration for all University computers.
- The occurrence of repeated instances of OS integrity problems may result in the removal of administrator-level access in order to prevent continued challenges in supporting the computer.

3.6 Definitions:

Administrator access level allows the user to have complete and unrestricted access to the computer. This includes the ability to install any hardware or software, edit the registry, manage the default access accounts and change file-level permissions. Manipulating these may cause serious stability issues with the workstation.

General access level allows most administrative powers with some restrictions. Installation of software or hardware that makes changes to the underlying operating system will require the assistance of CCS. General Access Level will generally assure the highest level of stability for a computer.

4 SUSL.ICT.2021.3 - Usage Policy of Computer Centers

ICT Policy Document **Centre for Computer Studies** **Sabaragamuwa University of Sri Lanka of Sri Lanka**	**Published Date:**	**Policy No:** **SUSL.ICT.2021.3**
Policy: Usage Policy of Computer Centers	**Approval Date:**	**Page No:**
Objectives: This policy aims to ensure about functioning the computing labs its maximum effectiveness for the users		

Responsible Official	
Responsible Office	
Signature	

4.1 Executive Summary:

Sabaragamuwa University of Sri Lanka of Sri Lanka maintains computing labs for academic, instructional, research, administrative and public service purposes. This policy is in place to ensure that the computing labs are kept functioning at an optimal level of effectiveness for all users.

4.2 Scope:

All persons using the university computer labs and equipment must abide by this policy. Violation of these policies may result in loss of computer lab privileges and other disciplinary action as described in the circulars issued by the University/University Grant Commission to students, faculty, and staff.

4.3 Policy:

- Persons using laboratory equipment must have a University ID card valid for the current semester or year and must be able to produce the card upon request by the authorized person.
- University computer labs must be used in a manner consistent with the policies of the university including the “Acceptable Use Policy”.
- All persons using the lab are responsible for backing up their own data and protecting their own information.
- Food, beverages, tobacco use, weapons, firearms or animals, are prohibited in the labs.
- Audio output or sound playing devices are permitted only with the use of headphones for study purposes only.
- The use of two-way communication devices is prohibited in the labrotaries.

- Children are permitted in labs only if accompanied by the university staff.
- Games, videos that are part of class assignments can be used with the instructions given by the subject lecturer to the center coordinators. However, if there are some bandwidth problems, such sessions may be restricted by the CCS network administration.
- CCS lab equipment may not be used for business purposes or in any profitable venture.
- Disabling computers by disconnecting cables, removing hardware, applying software locks, or locking workstations will be considered vandalism and treated as such under university policy.
- Anyone violating these policies or disturbing others in any way will be asked to leave from the center by the coordinator or any other center staff member.
- Persons with special needs requiring special access to computer laboratory equipment may contact coordinator and should get the permission from the director of the CCS.

5 SUSL.ICT.2021.4 -Policy of Electronic Communication

ICT Policy Document **Centre for Computer Studies** **Sabaragamuwa University of Sri Lanka of Sri Lanka**	**Published Date:**	**Policy No:** **SUSL.ICT.2021.4**
Policy: Policy of Electronic Communication	**Approval Date:**	**Page No:**
Objectives: This policy aims to protect sensitive university data; and to ensure the successful delivery of communications via E-mail		
Responsible Official		
Responsible Office		
Signature		

5.1 Executive Summary:

The University e-mail system is an official means of communication. The university views communication via e-mail to constitute being duly informed for faculty, and staff. Reading e-mail and checking ’one’s e-mail is thus an obligation for all University staff, students. Having ’one’s university e-mail forwarded to an off-campus account does not alter this obligation.

The university e-mail system is a delivery system for communication and does not constitute a long-term storage system for documents delivered through e-mail. Therefore, the e-mail system ought not to be relied upon for the long-term retention of official records of the university. Storing such records may alternatively be accomplished by saving them to a CD, DVD, flash drive, or by printing them. Hence, it is essential to comply with applicable laws and University policies, to protect sensitive university data; and ensure the successful delivery of communications by and between the university, students, faculty, staff, patrons, alumni, government, and business partners while using e-mail.

5.2 Documents:

Documents created by any user for which one needs reliable storage should utilize the above media and not rely solely on a copy stored on a local hard drive. Alternatively, such documents may be printed and stored.

5.3 Privacy:

CCS of the university operates the e-mail system with full respect for privacy and confidentiality in accordance with relevant laws, regulations and university policy. The custodians (CCS) of the e-mail system must not inappropriately access or disclose the content of mail on the University e-mail system unless required by law to disclose such contents or in certain circumstances only with the permission of the university Vice Chancellor.

5.4 E-mail Accounts:

E-mail supports the educational, research, administrative, and outreach mission of the university by serving as a nonofficial form of communication for account holders within the

SUSL community. Individuals resigning from **University staff** will not have access to their university provided e-mail account effective on the date of resignation.

1. The User Account Creation process outlined in the University User Accounts and Password Policy will be followed to create an e-mail account for a user. The User Accounts and Password Policy also specifies the format of an e-mail identifier (ID) and the validity of an account.
2. Position-related accounts (e.g., dean-app, sar- exams, and info) are distributed in addition to an e-mail account issued to a person based on his or her legal name or registration number (in the case of students) with the aim of unifying and archiving correspondence regardless of the individual who plays that role at any given time.
3. Some users may be affiliated with the university in more than one way. A faculty member who is also an alumnus, a staff member who may be a student, and a faculty member who is also a center director, for example. Multiple accounts can be provided to an individual who has multiple roles. In such cases, the respective account must be used for the appropriate communication. For example, a staff member who is a student should use his/her student account to engage with the research supervisor
4. Administrative e-mails for a ’user’s position must come from the role-based account. When one leaves a spot, those accounts must be passed on to the next in without removing or deleting any previous official communications and related stuff.
5. Departments, divisions, and projects may have their own e-mail under sub-domains of the university subject to the prior approval of the Director, CCS. In such cases, relevant policies need to be developed by the respective department, division, and project in line with this policy.

5.4.1 Use of e-mail

1. Those who have been given a university e-mail address are required to review it on a regular basis in order to obtain university communications.

2. All users must use their username@(subdomain).sab.ac.lk e-mail address for all official university correspondence. The role-based username must be used for role-specific communication.

3. All e-mail accounts must be used in accordance with the University Acceptable Use ’Policy’s Permitted and Prohibited Activities (AUP).

4. The use of e-mail to communicate study or business sensitive data is strongly discouraged at the university. When responding to or forwarding e-mail messages, users should exercise caution to avoid inadvertently disclosing confidential information. Furthermore, all potentially sensitive attachments must be encrypted and password-protected with a sufficiently complex password (as outlined in User Accounts and Password Policy). Offline, the password must be safely exchanged (i.e., through other means than e-mail).

5. All university-related e-mail received on a personal/external account should be forwarded to the ’recipient’s university-issued e-mail account. The recipient should also inform the sender that future correspondence should be sent via university e-mail.

6. No university-issued e-mail address can be used to create a profile on social media or other online tools utilized for personal use.

5.5 Privacy and Laws

1. The contents of all university-issued e-mail accounts are the property of the university, not the account holder.
2. The university retains the right to track e-mail to ensure compliance with relevant laws and university policies, as stated in the AUP. The university also retains the right to access and review all electronic information sent through or stored in e-mail, as well as to release information to third parties when necessary.
3. An e-mail produced or received by a university e-mail account in the course of the ’university’s official business is considered a public record and is subject to inspection and copying in compliance with national law.
    a. Although e-mails sent or received for personal use are usually not considered public records, they do not come under the scope of public records simply because they are stored on a government-owned computer system. Personal

e-mails that are found to be in breach of university policy can become public record as part of an investigation if the university discovers any abuse of the e-mail system.

b. If a university e-mail account is compromised, the corrective steps outlined in the Information Security Policy will be taken as soon as possible. Accounts that show a pattern of compromise will be suspended until an investigation is completed. The account holder will be required to complete adequate training if this is the case.

5.6 Log Retention:

DHCP and IP logs are retained for one week/month.

5.7 Definitions:

DHCP - Dynamic Host Configuration Protocol - Used by network devices to obtain the parameters required for operation in an Internet Protocol network

IP Address - Internet Protocol - The address of the client on the internet. Essentially identifies the client making any given connection to a site. Every computer connected to the internet has an IP address which enables the identification of that computer.

6 SUSL.ICT.2021.5 -Policy of Incident Response on Information Security

ICT Policy Document **Centre for Computer Studies** **Sabaragamuwa University of Sri Lanka of Sri Lanka**	**Published Date:**	**Policy No:** **SUSL.ICT.2021.5**
Policy: Policy of Incident Response on Information Security	**Approval Date:**	**Page No:**
Objectives: The aim of this policy is to respond to incidents that threaten the confidentiality, integrity, and availability of university digital assets, information systems, and the networks that deliver the information		

Responsible Official	
Responsible Office	
Signature	

6.1 Executive Summary:

The purpose of this policy is to provide the basis of appropriate response to incidents that threaten the confidentiality, integrity, and availability of university digital assets, information systems, and the networks that deliver the information.

6.2 Scope:

The Information Security Incident Response Policy applies to all users of the university Local Area Network.

6.3 Policy:

Responsibilities and standard operation procedure are establishing to ensure a quick, effective and orderly response to security incidents.

6.3.1 Objective

The objectives for incident response management should be agreed upon with the university and the Director, CCS, and it should be ensured that those responsible for understanding the organization’s priorities for handling Security Incidents.

Security Events should be reported through appropriate management channels as quickly as possible.

6.3.1.1 Examples of Security Incidents:

- The theft of physical loss of computer equipment.
- Loss or theft of mobile device.
- A server known to have sensitive data is accessed or otherwise compromised by an unauthorized party.
- A DDoS (Distributed Denial of Service) attack.

- The act of violating an explicit or implied security policy.
- A virus or worm uses open file shares to infect from one to hundreds of desktop computers.
- An attacker runs an exploit tool to gain access to a University 'server's password file.

6.4 Policies and Laws

1. Usage Policy of Computer Centers
2. Web Privacy Statement Policy

Since these policies interact and are applied together, a particular case should be understood in this policy as well as all other relevant and accepted policies. The university community must also be mindful of behavior that could violate national laws, resulting in civil or criminal court proceedings and penalties for which they may be held legally liable.

1. Computer Crimes Act No. 24 of 2007 of Sri Lanka
2. Electronic Transaction Act No. 19 of 2006 of Sri Lanka

7 SUSL.ICT.2021.6 -Network Protection Policy

ICT Policy Document **Centre for Computer Studies** **Sabaragamuwa University of Sri Lanka of Sri Lanka**	**Published Date:**	**Policy No:** **SUSL.ICT.2021.6**
Policy: Network Protection Policy	**Approval Date:**	**Page No:**
Objectives: The aim of this policy is to maintain, protect and ensure network and related technologies in an appropriate manner		
Responsible Official		
Responsible Office		

Signature	

7.1 Executive Summary:

The university network is organized as a series of local networks with protected zones where appropriate and accessible segments to encourage creativity and meet the needs of students, faculty, and researchers. The hardware and software that constitute Sabaragamuwa University of Sri Lanka Local Area Network are vital to the operation of the university. Viruses, malware, computer vulnerabilities and inappropriate use of the network are a threat to these resources and can detrimentally affect the ability to accomplish the ’institution’s mission. Because of the ’university’s dependence on the internet and related technology, as well as the need to communicate with the rest of the world, the network adheres to Internet standards established by higher education communities such as LEARN. The university has a responsibility to maintain these resources and ensure they are used in an appropriate manner.

7.2 Scope:

The Network Protection Policy applies to all users of the Sabaragamuwa University of Sri Lanka Local Area network.

7.3 Policy:

Sabaragamuwa University of Sri Lanka has the responsibility to protect valuable network resources and the confidentiality of sensitive personal information from any and all threats. In keeping with this responsibility, The University scans computer hardware devices connected to the Sabaragamuwa University of Sri Lanka Local Area Network for key security vulnerabilities. Where sufficient cause has been found to indicate a threat to the network, a threat to the university or a violation of public law, The University may disable the network access of the offending hardware device. Any attempt by a user to circumvent the system or process of scanning for key security vulnerabilities is a violation of this policy. Use of the Sabaragamuwa University of Sri Lanka Local Area Network constitutes the ’user’s acceptance of this policy.

7.3.1 Network Cabling

Category 6 (Unshielded Twisted Pair) UTP is used for horizontal station wiring to connect desktops, servers, networking equipment, IP phones, and IP cameras. To ensure interoperability and to make use of existing wiring, other types of network wiring used to connect specialized devices should use Category 6 UTP wherever possible. The T568B Wiring Standard must be followed when wiring RJ45 modular plugs. Fiber optic cabling will be used to link university buildings in order to improve bandwidth, quality of service, and surge safety. Each building should be linked to the network distribution switches at the CCS through a separate fiber where pathways allow.

To ensure interoperability, optimal use of the core network, and compliance with cabling and safety requirements, all major network wiring projects within a building, network wiring across floors of a building, and network wiring between buildings must be approved by the Director, CCS.

7.3.2 Networking Hardware

Switches, routers, wireless access points, wireless controllers, firewalls, and other network equipment are examples of network hardware. A UPS with at least 15 minutes of backup power should be used to power network hardware. Both network hardware should be secured and ventilated in a floor or wall-mounted lockable rack. CCS personnel should have physical access to all networking equipment connected to the university network 24 hours a day, 7 days a week to ensure proper operation and configuration. To ensure the protection, security, and privacy of equipment, data, and users, a protocol for such access must be negotiated and decided upon in advance with the respective head of the department, division, or project.

During each procurement cycle, network hardware should be examined for performance and security, and replacement decisions should be made based on the 'device's value, cost, and financial resources. To ensure interoperability, optimal efficiency, and compliance with networking and security requirements, relevant approvals from the Director, CCS should be obtained prior to procurement.

7.3.3 Internet Connectivity

All faculty, students, staff, and approved project personnel have access to the internet, as specified by the ““Acceptable Use Policy”. Users should not use social media or access leisure websites during working hours, and they should not abuse university network services.

7.4 Definitions:

The Sabaragamuwa University of Sri Lanka Local Area Network is the group of stations (computers, telephones, printers or other devices) owned or operated by the university connected by communications facilities owned or operated by the Sabaragamuwa University of Sri Lanka for exchanging information. The connection can be permanent, via cable, or temporary, through telephone or other communications links. The transmission medium can be physical (i.e. fiber optic cable) or wireless (i.e. satellite).

8 SUSL.ICT.2021.7 -Password Policy

ICT Policy Document **Centre for Computer Studies** **Sabaragamuwa University of Sri Lanka of Sri Lanka**	**Published Date:**	**Policy No:** **SUSL.ICT.2021.7**
Policy: Password Policy	**Approval Date:**	**Page No:**
Objectives: The aim of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change of passwords.		
Responsible Official		
Responsible Office		
Signature		

8.1 Executive Summary

Passwords are an important aspect of computer security. A poorly chosen password may result in the compromise of Sabaragamuwa 'university's entire network. The purpose of having a password policy is to ensure a more consistent measure of security for Sabaragamuwa University of Sri Lanka Local Area Network and the information it contains. The implementation of this policy will better safeguard the personal and confidential information of all individuals and organizations affiliated, associated, or employed by the university. Additionally, this policy establishes a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change of passwords.

8.2 Scope

The Password Policy applies to all persons accessing the Sabaragamuwa University of Sri Lanka Local Area Network regardless of their capacity, role or function. Such persons include students, faculty, staff, third party contractors, visitors (guests), consultants and employees fulfilling permanent, temporary or part-time roles.

8.3 Policy

- Users must not reveal their passwords to anyone, including CCS and other administrative personnel.
- Students must not reveal their usernames and passwords to anyone.
- Users should not share or change the common passwords that given to access to online library services, and electronic library resources.
- Users should not send passwords via e-mail or phone, and should not save passwords in applications like web browsers and mobile apps that have a remember password feature.
- Users with access to multiple user accounts (depending on their position and the services they access) should not use the same password for both university and non-university accounts.
- Users must not knowingly participate in any action with the intent of obtaining other 'users' passwords.

- Users must use their usernames and passwords to access SUSL ICT facilities.
- If a password breach is suspected, a user must update his or her password immediately and notify the appropriate systems administrator.
- Users must pick and maintain a safe password, as well as log off after using ICT services, according to the instructions given by the appropriate systems administrators and the University password policy.

In addition to passwords, other forms of authentication such as fingerprints, access cards and tokens (magnetic strip and NFC based ones), device signing, and digital certificates may be used for specialized applications. In such cases, due care should be used to issue, transfer, use, and store those credentials similar to that of a password.

1. Password Creation

A password should be an alphanumeric string consisting of characters, numbers, and symbols in the format specified below. Moreover, an acceptable password for an account must also satisfy the following requirements:

1. Not be a password that is one of the three (3) most recently used passwords for that account
2. Must not be a dictionary word, slang, dialect, or jargon

All information systems should be configured to enforce all initial and renewed passwords to satisfy this policy.

Table 1: Password complexity matrix.

Account Type	Minimum Length	Combination	Change Frequency	Reset Mechanism
Faculty and administrative staff member	8	At least 1 uppercase(A-Z) and one lowercase(a-z) character, 1 number (0-9), and 1symbol	Annual	Self-service reset if valid mobile and secondary e-mail are set up at the time of registering.
Undergraduate student accounts			Annual	Self-service reset if valid mobile and secondary e-mail are set up at the time of registering.
Postgraduate student accounts				

Visitor accounts including visiting lecturers			Annual	Self-service reset if valid mobile and secondary e-mail are set up at the time of registering.
Role and task specific accounts			180 days	On written request of respective head of department
Event and project specific accounts				
Systems Administrators	12		Annual	At service desk or on the written request of the user and approved by head of department/division

Systems Accounts / Super user/ User			180 days	By super user
Passwords used to protect encryption keys	15		Annual	

8.4 Policies and Laws

This policy is supplemented by the following policies:

1. Acceptable Use Policy
2. Password Policy
3. Web Privacy Statement Policy
4. Social Media Policy
5. E-Learning Policy

Since these policies interact and are applied together, a particular case should be understood in this policy as well as all other relevant and accepted policies. The university community must also be mindful of behavior that could violate national laws, resulting in civil or criminal court proceedings and penalties for which they may be held legally liable. Some of the legislated acts of parliament in this respect are:

1. Computer Crimes Act No. 24 of 2007 of Sri Lanka
2. Electronic Transaction Act No. 19 of 2006 of Sri Lanka
3. Electronic Transactions (Amendment) Act, No. 25 of2017

9 SUSL.ICT.2021.8 -Web Privacy Statement

ICT Policy Document **Centre for Computer Studies** **Sabaragamuwa University of Sri Lanka of Sri Lanka**	**Published Date:**	**Policy No:** **SUSL.ICT.2021.8**

Policy: Web Privacy Statement	**Approval Date:**	**Page No:**
Objectives: The aim of this is to let user knows what personally identifiable information collected when the user visits the website and use such information		
Responsible Official		
Responsible Office		
Signature		

9.1 Executive Summary

Sabaragamuwa University of Sri Lanka of Sri Lanka has adopted this Web Privacy Statement in order to inform users of the university policies with respect to information collected on this website.

9.2 Privacy

The university is committed to respecting your privacy and recognizing your need for appropriate protection and management of the personally identifiable information you share with us. The purpose of this Privacy Statement is to let you know what personally identifiable information we may collect from you when you visit the website, how we use such information.

9.3 Information We Collect

There are three types of information that may be collected during your visit: Network traffic and Web server logs, cookies, and information voluntarily provided by you.

Network Traffic and Web Server Logs

In the course of ensuring network security and consistent service for all users, the university may use software programs to do such things as:

- Analyze network traffic
- Identify unauthorized access
- Detect computer viruses and other software that might damage University computers or the network
- Monitor and maintain the performance of the University network

In the course of such monitoring, these programs may detect such information as e-mail headers, addresses from network packets and other information. Information from these activities is used solely for the purpose of maintaining the security and performance of the 'university's networks and computer systems. Personally, identifiable information from these activities is not released to external parties unless required by law.

The University Web servers collect and store information from Web site visitors to monitor Web site performance and to improve service. This information includes the following:

- Page visited
- Date and time of the visit
- Domain name or IP address of the referring site
- Domain name and IP address from which the access occurred
- Version of browser used and the capabilities of the browser

The university makes no attempt to identify individual visitors from this information: any personally identifiable information is not released to external parties unless required by law.

9.4 Cookies

Cookies are small bits of data stored on the hard drive on behalf of a Web site and returned to the Web site on request. This site may use cookies for two purposes: to carry data about your current session at the site from one Web page to the next, and to identify you to the site between visits. If you prefer not to receive cookies, you may turn them off in the browser, or may set the browser to ask you before accepting a new cookie. Some pages may not function properly if the cookies are turned off. Unless otherwise notified on this site, we will not store data, other than for these two purposes.

9.5 External Links

Sabaragamuwa University of Sri Lanka sites provide links to other World Wide Web sites or resources. We do not control these sites and resources, do not endorse them, and are not responsible for their availability, content, or delivery of services. In particular, external sites are not bound by the ’university’s Web privacy policy; they may have their own policies or none at all.

10 SUSL.ICT.2021.9 - Social Media Policy

ICT Policy Document **Centre for Computer Studies** **Sabaragamuwa University of Sri Lanka of Sri Lanka**	**Published Date:**	**Policy No:** **SUSL.ICT.2021.9**
Policy: Social Media Policy	**Approval Date:**	**Page No:**
Objectives: The aim of this policy is to make opportunities to interact with the university community and jeopardize the ’university’s credibility, sensitive and proprietary information,		
Responsible Official		
Responsible Office		
Signature		

10.1 Executive Summary:

Social media offers a one-of-a-kind and diverse set of opportunities for interaction with the University community and beyond. Improper usage, on the other hand, could jeopardize the ’university’s credibility, sensitive and proprietary information, and legal and regulatory enforcement. These questions apply to users’ personal accounts as well, since you will be identified as a student, faculty member, staff member, or associate of the university

10.1.1 Creation of Social Media Sites

1 The SUSL will be communicated via social media platforms, which will represent the ’university’s broad values and culture. A coherent and recognizable portrayal of the university is of paramount importance because it will be easily identifiable as a part of the university.

2 The university social media pages are the responsibility of the Director, CCS (or their nominee).

3 This includes the ’university’s official social media sites (including content repositories like WiKis and Forums for Staff and Students), as well as University profile pages on third-party sites like Facebook, Twitter, LinkedIn, and YouTube.

4 Third party sites (Facebook, Twitter, LinkedIn, and YouTube) are mainly design under the university and the associate pages are created for the faculties and the departments.

5 The university blog will be used to share the articles of the university community and to share the e books for the readers available in the library.

6 Only the content provider (i.e., respective Heads/Deans/Directors of the department/division) may request through the Director, CCS to web coordinator of the relevant faculty to set up a SUSL organizational unit social media site for the department, division, or project. The request should include the following:

a. The contact details of the content owner and content developers/moderators.

b. The reason for having a separate account/presence that is different from the existing university social media sites.

7 The establishment and maintenance of such a faculty, department, division, University projects, subject associations and students clubs/circles social media page or channel may be delegated with the permission from the respective Heads/Deans/Directors to the web committee of the relevant faculty.

10.1.2 Personal Accounts on Social Media Sites

1. Users should use third-party social media sites like Facebook, Twitter, YouTube, and LinkedIn at their own risk. Since the university has no power over these pages, it cannot be held liable for any data stored on them.
2. In addition to the rules outlined in this Policy and AUP, users should familiarize themselves with the terms and conditions that govern each social networking platform and follow them.
3. While the SUSL does not prohibit private use of social media, it is necessary to remember that the same professional standards, rules for communicating with students, alumni, the media, and other university constituents, and national laws apply online as they do in person. You are responsible for anything posted on your personal social media sites.
4. representing SUSL both inside and outside of your classroom and office as a student, faculty, or staff member
5. Users should protect themselves by reading and being familiar with the privacy policies regulating the social media platform to ensure that they support any data disclosures that might be made. It is strongly advised that users keep their privacy settings on such pages as high as possible (e.g., a private profile on Facebook)
6. Think about what ’you’re going to post before you do it. And after a ’user’s social media account has been deactivated, copies of the ’user’s details can still be available on the internet. As a result, users should think about the long-term online footprint they are leaving before uploading content.

10.1.3 Social Media Content Access, Creation, and Sharing

1. All requests for updates or new posts to a ’university’s social media site must go through the Director, CCS (or their nominee) and will be considered on a case-by-case basis.
2. Accessing, creating, and sharing content related to the university and

personal social media sites must comply with the Permitted and Prohibited Activities as specified in the University Acceptable Use Policy (AUP).

3. Users are encouraged to use their department, division, or project social media platforms to communicate responsibly at all times, with due respect for the ’University’s and ’others’ rights and reputations, as described in the AUP.
4. All University social media sites must identify themselves as members of the University administration.
5. Use of the University logo and branding on department, division, or project social media sites is subject to the University branding guidelines.
6. Each social media site must contain contact details of the department, division, or project, as well as an e-mail address that is regularly followed up by the web content creator or web coordinator. Web coordinator (or their nominee) is responsible for monitoring and maintaining the site and should check the sites/e-mails for new posts/comments at least once a week.
7. The committee for the content creation and sharing through the social media should be created by every faculty including the Dean, department heads, web coordinator, English lecture or instructor and selected nominees to make the content creatively, decide what photos or images should be published and the time frame of the news should be published through the social media.
8. Time calendar with news and events should be presented to the Faculty board in every month and should get the approval before sending to the Director, CCS.
9. All messages posted by followers must be moderated before appearing on any University social media site. Any posts/comments that are illegal, obscene, defamatory, harassing, discriminatory, threatening, infringing on the intellectual property rights of others, an invasion of privacy, or violation of AUP must not be published.
10. All University social media pages should meet the goals of high quality in

both style and presentation. All social media sites must be regularly updated with at least one post per month. While the language used can fit the style of the particular social media platform, care must be taken to preserve the semantics of the message, and not to have obvious grammar and spelling errors

11. University strongly urges that faculty, instructors, supervisors, and managers not ask to be a part of a student’s or subordinate’s social media network. Any student, faculty, or staff may reject, without fear of retaliation, any request from any other student or employee that, if accepted, would permit access to a private social media site or page.

10.1.4Policies and Laws

This policy is supplemented by the following policies:

1. Acceptable Use Policy
2. Password Policy
3. Web Privacy Statement Policy
4. Social Media Policy

Since these policies interact and are applied together, a particular case should be understood in this policy as well as all other relevant and accepted policies. The university community must also be mindful of behavior that could violate national laws, resulting in civil or criminal court proceedings and penalties for which they may be held legally liable. Any of the laws have been enacted. Some of the legislated acts of parliament in this respect are:

1. Computer Crimes Act No. 24 of 2007 of Sri Lanka
2. Electronic Transaction Act No. 19 of 2006 of Sri Lanka
3. Electronic Transactions (Amendment) Act, No. 25 of 2017

11 SUSL.ICT.2021.10 - E-Learning Policy

ICT Policy Document **Centre for Computer Studies** **Sabaragamuwa University of Sri Lanka of Sri Lanka**	**Published Date:**	**Policy No:** **SUSL.ICT.2021.10**
Policy: E-Learning Policy	**Approval Date:**	**Page No:**
Objectives: The aim of this policy is to manage E-Learning activities of Sabaragamuwa University of Sri Lanka of Sri Lanka with the equal quality and standards as its conventional programs and protect E-Learning activities from any potential risks posed by the challenges and complexities in conducting such programs		
Responsible Official		
Responsible Office		
Signature		

11.1 Executive Summary:

E –learning comprises all forms of electronically supported learning and teaching. E-learning is essentially the computer and network-enabled transfer of skills and knowledge. E-learning applications and processes include Web-based learning, computer-based learning, virtual education opportunities and digital collaboration. Learner’s access primary content and instruction from an e-learning environment using a variety of tools including, but not limited to, e-mail, text and voice chat, discussion boards, web pages, and multimedia technologies. Specific technologies employed will vary by course and instructor. SUSL has implemented Learning Management System (LMS), remote learning facilities through the Lanka Education and Research Network (LEARN) , Virtual Learning Environment (VLE) for students and staffs to carry out their academic activities and Examination Virtual Learning Environment (EVLE) for conducting examinations through the faculties.

11.2 Scope

This E-Learning policy applies to help manage the E-Learning activities of Sabaragamuwa University of Sri Lanka of Sri Lanka with the equal quality and standards as its conventional programs. Further, this policy aims at protecting E-Learning activities from any potential risks posed by the challenges and complexities in conducting such programs.

11.3 Policy

- SUSL ensures that its eLearning provision can meet the needs of a full range of flexible and independent learning experiences. This includes on and off-campus learners in local and regional settings and covers both blended and fully eLearning courses ranging from full awards to informal and individual learning.
- SUSL ensures that students taking eLearning courses have equity of opportunity as they are in the university premises are fully aligned to the needs of the e-Learner.
- SUSL ensures that eLearning activities have coherence, consistency and transparency the programs are internally coherent and consistent in the way the objectives, content, student activity and assessment, match to each other. It is open and accessible in its design.
- SUSL continually works towards ensuring that all systems, both manual and electronic, used in the eLearning context interoperate in the most effective way to provide learners with a effective and increasingly individualized learning environment encompassing all aspects of their experience as a student of the university, as part of a holistic Managed Environment for Learners.
- SUSL exploits the range of technologies used in the eLearning context to work with partner organizations, employers and individuals to assist it in meeting its goals of supporting the independent and lifelong learner and continuing professional development.
- SUSL, through its quality processes, ensures that eLearning.
- Provision meets the standards expected by the university, funding bodies and relevant legislation, and that it is accessible, educationally sound, engaging and appropriate to its target population.

- SUSL provides zoom accounts for the lecturers which is provided by the LEARN and the policies related to the zoom accounts are created by the LEARN and SUSL is adhering those policies for the zoom accounts as SUSL policies for zoom accounts. Any unauthorized or malfunctioned activity related to zoom accounts will be acknowledged according to those policies.
- Education roaming (eduroam) which is an international Wi-Fi internet access roaming service for students and the staff will be provided through LEARN. This will be named as LEARN eduID with lifelong learning, research, and collaboration with a number of research institutions and companies. This is safer and easier because it is connected to a real individual using one username and password. The policies which are related to eduID will be as same as LEARN policies.

11.3.1 Virtual Learning Environment (VLE)

SUSL's VLE is based on the Moodle Learning Platform and with these systems, each faculty/department/center facilitates students to access course contents, materials online. The student and staff login information is submitted by the relevant faculty/department/center and for further inquiries, contact the coordinator or the director CCS. User accounts of staff and students for the VLE are created by the Director, CCS according to the request of the relevant department or the faculty through the coordinator of that faculty. There is a separate virtual environment for conducting examinations and that is identified as EVLE.

11.3.2 LEARN

Lanka Education and Research Network (LEARN) had been in development over 30 years.

A National Research and Education Network (NREN) is usually a specialized Internet Service Provider dedicated to supporting the needs of the research and education communities within a country and it is distinguished by support for a high-speed backbone network, often offering dedicated channels for individual research projects. LEARN is an association registered under the Companies Act of Sri Lanka, and works as a specialized internet service provider for education and research purposes. It provides a high-speed backbone network connecting the Ministry of Education, UGC, and state higher education and research institutions. LEARN functioning as an internet service provider facilitated white listing university web servers for access to online tertiary education.

11.3.3 Role and responsibilities of the students

- The student is responsible for making their own arrangement for minimum necessary infrastructure support to resolve failures related to facilities.
- Students should ensure that they engage with learning materials and mode of delivery.
- The student should conform to the schedule for the program delivery and assessment, monitor the receipts of materials and alert the relevant lecturer or the coordinator, CCS if any material is corrupted or failed to arrive.

12 SUSL.ICT.2021.11 - Hardware and software disposal policy/ ICT asset disposal policy

ICT Policy Document **Centre for Computer Studies** **Sabaragamuwa University of Sri Lanka of Sri Lanka**	**Published Date:**	**Policy No:** **SUSL.ICT.2021.11**
Policy: Hardware and software disposal policy/ ICT asset disposal policy	**Approval Date:**	**Page No:**
Objectives: The objective of this policy is to ensure that all university-related information is adequately removed from information technology (IT) equipment prior to disposal and the disposal of IT equipment includes equipment being sold internally or externally, re-allocated to other departments within the university, trade-in to a vendor or supplier, return on end of lease, loan to any entity, donation or physical destruction of equipment including collection by rubbish revivalists.		
Responsible Official		
Responsible Office		
Signature		

12.1 Executive Summary:

The university has legal obligations to ensure that all computers, IT equipment, mobile phones, tablets and data storage media (e.g. USB drives, DVDs, CDs, etc.) including the data and software held upon such equipment, are disposed of appropriately and legally. To this end, members of the university must follow this policy for the reuse and disposal of computers and IT equipment.

12.2 Scope:

This policy applies to:

1. External Vendors contracted to physically cleanse IT equipment as part of the disposal process.
2. Organizational Units within SUSL who purchase or lease IT equipment.
3. Information Technology staff.
4. Desktop PCs, laptops/tablets, servers, smart phones and other electronic storage devices

12.3 Policy

The Center for Computer Studies shall have sole responsibility for selling, cannibalizing, donating, trashing, or otherwise disposing of computer technology. Departments shall turn over all obsolete, broken, or unwanted technology items to CCS for disposal.

12.4 Procedure

Departments wishing to dispose of unwanted technology items shall do so by calling in or e-mailing to Director, CCS and the location of the hardware in question.

12.4.1Removal of University Information

All university information including computer software, logos and data must be removed from IT equipment prior to disposal.

12.4.2Desktop and Laptop Computers

- All university information including computer software, logos and data is to be removed from PCs and laptops prior to disposal

- Where the PC or laptop is severely damaged and cannot be operated to achieve the removal of software, any storage media must be either removed physically and reformatted on another PC or physically destroyed.
- The university must retain relevant documentation and licensed software media unless allowed by the license conditions, for example, software used under a site license.

12.4.3 Servers

1. Backup of Information

As servers often contain data and information used by the whole University community it is vital to ensure that this is archived at the time the machine is taken out of production service.

2. Removal of University Information.

Removal of all university related information is to be completed by physically wiping any hard disks on the server. If the operating system software license permits, the operating system can be re-installed.

3. Removal of other non-volatile memory
4. If a purchaser requires the presence of the operating system to verify the working condition of the hardware, the operating system must be set to its original default distribution state.
5. This process requires removing all SUSL generated data, applications, personal files of users and cleaning of selected files relating to passwords, groups, logs, mail boxes, print queues etc.
6. To maintain security of the network infrastructure, the disks must be erased.
7. Where the server is severely damaged, and cannot be operated, any storage media must be either removed and physically wiped on another machine or physically destroyed.

8. The university must retain relevant documentation and licensed software media unless allowed by the license conditions.

12.4.4 Other Devices

- All SUSL proprietary or otherwise confidential information must be removed prior to disposal. This can be achieved by resetting the device to the original factory default.

12.4.5 Leased Equipment

- Removal of University Information steps according to the type of device is to be undertaken prior to disposal.

CCS will dispose of items in the following manner, in order of preference.

- Trickle Down:

Hardware that has been removed from an office shall be installed elsewhere for low-end use where appropriate.

- Selling:

All hardware no longer of use to SUSL shall be sold wherever possible. CCS will ensure the hardware is cleared of all pertinent software and data. SUSL inventory tags shall be removed and attached to a “hardware disposal” document, which will be kept on file in CCS. The inventory database will be updated to reflect the removal of the hardware.

- Cannibalizing:

Hardware that cannot be sold and can no longer be used in whole, but has useful components, will be cannibalized for those components. SUSL inventory tags shall be removed from the shell and attached to a “hardware disposal” document, which will be kept on file in CCS. The inventory database will be updated to reflect the cannibalization of the hardware.

- Donating:

Hardware that cannot be sold and has no useful components will be donated where possible. SUSL inventory tags shall be removed from the shell and attached to a “hardware disposal” document, which will be kept on file in CCS. The inventory database will be updated to reflect the donation of the hardware.

- Trashing:

Hardware that cannot be sold, has no useful components, and is not worth donating, will be trashed. Many materials used in computer hardware can be recovered by recycling for use in future production. Reuse of tin, silicon, iron, aluminum, and a variety of plastics that are present in bulk in computers or other electronics can reduce the costs of constructing new systems. Components frequently contain lead, copper, gold and other valuable materials suitable for reclamation. SUSL inventory tags shall be removed from the hardware and attached to a "hardware disposal" document, which will be kept on file in CCS. The inventory database will be updated to reflect the trashing of the hardware.

13 SUSL.ICT.2021.12 - Web site use and update policy

ICT Policy Document **Centre for Computer Studies** **Sabaragamuwa University of Sri Lanka of Sri Lanka**	**Published Date:**	**Policy No:** **SUSL.ICT.2021.12**
Policy: Web site use and update policy	**Approval Date:**	**Page No:**
Objectives: The objective of this policy is to give a clear idea on the appropriate use of university web site among the staff, students and others and increase the usage of web site		
Responsible Official		
Responsible Office		
Signature		

13.1 Executive Summary:

CCS provides web hosting services to all University entities. Websites must be used to promote educational, academic, and professional programs that are in line with the university's educational objectives and policies. This section of the policy covers all types of University web presence, including those generated by the university, departments, employees, and students.

13.1.1 University Websites

1. University websites will represent the university's broad values and culture while conveying the SUSL brand. A coherent and recognizable portrayal of the university is of paramount importance because it will be easily identifiable as a part of the university.
2. SUSL is the sole owner of the university website *.sab. ac.lk. The domain *.sab.ac.lk is also owned by the university. University web presence must only be on *.sab.lk unless for advanced and accepted applications. Although certain members of staff will have access to edit certain parts of the website, add new content, and delete old content, the website and all of its sub-sites will remain the university's property.
3. The University website is the responsibility of the Director, CCS (or their nominee) and that responsibility has been decentralized to the web coordinators of the faculties for updating faculty web pages.
4. Only the content provider (i.e., respective Head/Director of the department/division) may request from the Director, CCS to set up a SUSL organizational unit website for the department, division, or project. Any requests for an e-website should include the following:
    a) The contact details of the content owner.
    b) The high-level structure of the website and what content will be presented on the website.
    c) The visual design of the website.
    d) Any special technical requirements for the site (databases, wikis, webservices, and APIs).
    e) Anticipated workloads such as types and sizes of content, users and their access patterns.
5. The establishment and maintenance of such a department, division, or project website may be delegated with the permission from the respective Head/Director to web coordinator.
6. The committee for the content creation and sharing through the university web should be created by every faculty including the dean, department heads, web coordinator, English lecture or instructor and selected nominees to make the content creatively, decide what photos or images should be published and the time frame of the news should be published through the web pages.

7. Time calendar with news and events should be presented to the faculty board in every month and should get the approval before sending to the Director, CCS.
8. To ensure consistent maintenance and application of patches and security updates all university websites must be hosted on the CCS-managed webservers.
9. Use of the university logo and branding on department, division, or project websites is subject to the university branding guidelines. Without any permission from the authorized parties, the university name and logo cannot be used in outside.
10. Each website must contain contact details of the department, division, or project, as well as an e-mail address that is regularly followed up by the web content creator or web developer.
11. Publications must include a statement of copyright and sharing policy when appropriate. When including copyrighted materials indicate that the permission has been received.
12. When web pages related to university journals, university conferences, magazines can be created through CCS without damaging the existing structure of the university/faculty website. If the organizers should want separate template of web pages for these, they should be provided acceptable strong evidence for requesting separate web page templates under LK domain. Then CCS will be provided separate template and the request should be done through Heads/Deans/Vice Chancellor to CCS.
13. CCS will be responsible for the archival of old data and information such as news, events, and publications with images.
14. All university web pages should meet the goals of high quality in both style and presentation. Web sites colors should be used according to the approved colors by the faculty boards of relevant faculties.
15. All websites must be regularly updated. Correct grammar and spelling are expected. According to the faculty pages, the content should be corrected with correct grammar and spelling checked by the English Instructor or Lecturer and shared with the web coordinator through the relevant department head, dean and the academic staff related the event.

13.1.2 Policies and Laws

This policy is supplemented by the following policies:

1. Acceptable Use Policy
2. Administrator Access Policy

3. Network Protection Policy
4. Password Policy
5. Web Privacy Statement Policy

Since these policies interact and are applied together, a particular case should be understood in this policy as well as all other relevant and accepted policies. The university community must also be mindful of behavior that could violate national laws, resulting in civil or criminal court proceedings and penalties for which they may be held legally liable. Any of the laws have been enacted. Some of the legislated acts of parliament in this respect are:

- Computer Crimes Act No. 24 of 2007 of Sri Lanka
- Electronic Transaction Act No. 19 of 2006 of Sri Lanka
- Electronic Transactions (Amendment) Act, No. 25 of 2017

This policy is prepared by a committee appointed by the Senate Standing Committee on Quality Assurance, SUSL (28th SSC-QA, held on April 2021) and the composition of the committee is as follows,

Mr. R.L. Dangalla (Chairman of the committee & Director, Centre for Computer Studies)
Mr.S.P.K. Ranathunga (Member)
Mr. R.M. Nevil B. Rathnayake (Member)
Prof. B.T.G.S. Kumara (Member)
Prof. H.A.D. Ruwandeepika (Member)
Ms. P.G.I. Dias (Secretary)

Centre for Quality Assurance,

Sabaragamuwa University of Sri Lanka

September 2021.

********This policy has been approved at the 256th Senate and 278th Council***