South Eastern University of Sri Lanka

Acceptable Use Policy for ICT

1. Objective

The objective of this policy document is to outline the acceptable use of South Eastern University of Sri Lanka (SEUSL) Information and Communication Technology (ICT) Resources by all users and the unacceptable use that would expose the University to risks that include loss of confidentiality, damage to reputation, malware attacks, compromise of network systems and legal issues.

2. Scope

The policy is applicable to all users of ICT Facilities and ICT Resources managed by the South Eastern University of Sri Lanka (SEUSL).

3. Definitions

ICT Facility means any South Eastern University of Sri Lanka (SEUSL) owned or operated installation or building such as data center, server room or network room that contains critical University ICT Resources;

ICT Resource means any form of University-controlled technology used to collect, process, store and disseminate information, including but not limited to:

Phones (including mobile devices) and supporting equipment, voice mail, SMS;

Smartphones, tablets;

Servers, desktops and laptop computers;

Email, collaboration tools (including, instant messaging, video conferencing) facsimile (fax);

Any connection to the University's network, or use of any part of the University's network to access other networks;

All University supplied software;

All other hardware including, printers, scanners, etc.;

Any off-campus computers and associated peripherals and equipment provided for the purpose of University work or associated activities;

Usage of remote systems accessed via University ICT Facilities.

User any person accessing any of the University's ICT resources and / or facilities, including, but not limited to – staff, students, alumni, consultants, contractors, third parties, other users who are authorized by the University authority to access systems and/or the campus network, and anyone connecting from outside the -South Eastern University of Sri Lanka equipment (e.g. laptop computers) to the University network.

4. Legislative Framework

Use of University ICT Resources must comply with all relevant computer, data protection, cyber related and criminal laws in Sri Lanka and abroad; all University rules and policies; and all relevant contracts and licenses.

Computer Crime Act, No. 24 OF 2007

Penal Code (Amendment) No. 22 of 1995

: Section 286A – Introduced offences to ensure Child Protection. Can be

extended to online child abuse images (Meets minimums requirements under

Article 9 of the Budapest Cybercrime Convention)

Penal Code (Amendment) Act No. 16 of 2006

: Introduces an offence – Requiring all persons providing Computer service to

ensure that the service is not used for sexual abuse of children.

Payment Devices Frauds Act No. 30 of 2006
:An Act to prevent the possession and use of unauthorised payment devices

(deals with credit card frauds)

Other International Computer, Data Protection, Cyber related laws.

Employer/Employee Obligations under the existing Collective Workplace Agreement;

The University's academic integrity, sexual harassment, racism, bullying and equal opportunity policies and/or statements.

5. Acceptable Use of ICT Resources

Users are required to:

Accept full responsibility for their use of ICT Resources in accordance with all relevant University policies;

Avoid consuming an unreasonable amount of available ICT Resources (e.g. consuming an amount that would negatively impact the experience of other users);

Only access ICT Resources for which they are authorized;

Report any damage to ICT Resources to an appropriate member of staff;

Take precautions to ensure that screens displaying sensitive or critical information are not seen by unauthorized persons in public areas;

Be responsible for all activities originating from their accounts (e.g. student registration number, staff / employee number);

Comply with the terms and conditions of any licensed third-party applications.

Users are not permitted to:

Copy, download, store or transmit material which infringes copyright, including music files, movies or videos, or pirated software;

Create or transmit any material that could reasonably be deemed offensive, obscene or indecent, intimidating or distressing (other than for approved teaching, research or incident investigation purposes);

Create or transmit any material that is likely to discriminate, harass or is defamatory;

Create or transmit any material that is confidential and for which there is no authority to transmit;

Avoid connecting untrusted removable storage media to University-owned mobile computing devices;

Use ICT resources for unauthorized commercial activities, private or financial gain to a third party;

Send junk-emails, for-profit messages, chain letters or unsolicited commercial emails (SPAM);

Connect any network equipment to the University network (e.g. modems, mobile internet, mobile data card) that will extend access or provide off-campus access to ICT Resources without approval;

Subvert security by creating or installing any form of malicious software (e.g. worms, viruses, sniffers) or hardware (e.g. NIC, pen drive etc.) which may affect computing or network equipment, software or data;

Subvert security by attempting unauthorized access to any ICT Resource.

5.1. Acceptable Use of the Internet

Internet connectivity along with other internet services are provided to the users of the South Eastern University of Sri Lanka for learning, research, teaching and the provision of administrative purposes. All individual Internet access activity will be automatically recorded and monitored; this includes pages viewed, files and programs transferred (including user date and time of access).

Users must not access any pornographic, racially insensitive and/or similar material (other than for approved teaching or research purposes);

Users must not use the internet to attempt to gain unauthorized access to other systems;

Users who engage with social media in the context of the University should obtain the approval of the governing authority of the university.

5.2. Acceptable Use of Email

The University email service is provided to all Users for official purposes. The following rules must be adhered to by the Users:

All e-mail received, created and sent using the @seu.ac.lk address are deemed official University correspondence, are subject to the rules and regulations of the university and related Acts and remain the property of the University;

Whilst some personal email usage is permitted, all email content remains the property of the University;

E-mails containing sexist, racist, offensive or abusive material are not acceptable under any circumstances;

If an offensive e-mail is received it must not be distributed to others and must be reported immediately.

Users must not send e-mail which may compromise the reputation of the University such as harassment or chain letters, pornographic or insensitive material, or knowingly send e-mail with attachments that may contain viruses, worms, or malicious content;

Users must not knowingly open any attachments or links which are suspicious or from untrusted or unknown sources;

Users must not send e-mail impersonating someone else.

5.3. Acceptable Use of Collaboration Services (Social Networks: Facebook, Viber, WhatsApp, Google docs, Microsoft 365, E- Mail Remote Desktop, Team Viewer etc.)

The University's collaboration tools are provided to all Users for a University purpose. The following rules must be adhered to by Users of the services:

All instant messages received, created and sent using the University's collaboration tools are deemed official University correspondence, are subject to the rules and regulations of the university and related Acts and remain the property of the University;

Instant message functionality is not a replacement for email and as such any formal documents or official communications should be via email only;

Sensitive or proprietary information must not be shared using instant messaging or video conferencing services as the services are not designed for such purposes;

Users must not knowingly open any attachments or links which are suspicious or are received from untrusted or unknown sources via instant messaging;

Users must not use instant messaging for sharing personal, malicious or copyright file attachments that are not directly related their employment or studies;

Users must not send instant messages which may compromise the reputation of the University such as harassment, pornographic or insensitive material;

Users are reminded to be mindful when using available desktop sharing functionality not to expose sensitive or proprietary University information;

All use of instant messaging and video conference services are monitored and recorded. Information is stored and archived to meet University record retention requirements.

5.4. Acceptable Use of Phone Services

The University's phone systems are provided to staff for a University purpose. The following rules must be adhered to by Users of University phone services:

Users must not misuse phone services to make harassing, insensitive or malicious phone calls;

Calls to premium telephone numbers or international numbers are not permitted unless approved by the University.

5.5. Personal Use (Non-University Use)

Acceptable use of IT permits the personal use of University ICT Resources if it does not:

Interfere with the performance of the user's job, studies or other University responsibilities;

Interfere with normal IT operations;

Interfere with the use or access of other users;

Include use of an application on a device which does not belong to a University staff member;

Damage the reputation or operations of the University; and

Impose unreasonable additional costs on the University.

6. Compliance and Enforcement

Authorities of the university including the Security Services are responsible for monitoring user compliance with this policy and investigating and reporting breaches of this policy.

Heads of the Faculties /Departments / Units / Centers / Divisions are responsible for reporting any security incidents or breaches of this policy by staff under their supervision to the ICT Center.

Users are responsible for reporting any security incidents and breaches of this policy to the ICT Center.

Failure by Users to comply with any element of this policy may result in disciplinary action in accordance with the relevant disciplinary procedures.

In addition to imposing any penalty or disciplinary action, the University may act to recover the costs associated with any damage to or loss of IT resources and/or data caused by an individual through the deliberate breach of this policy. Cases of serious, deliberate or criminal breach may be referred to external authorities and may result in civil or criminal proceedings.

Last updated: 20.01.2016

Contact:

South Eastern University of Sri Lanka

University Park,

Oluvil, #32360,

Sri Lanka.

Telephone: +94 67 2255062 /63 /64

FAX: +94 67 2255217

Website: www.seu.ac.lk