SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY,

IT SERVICES DIVISION

USE POLICY FOR IT RESOURCES

VERSION 1.1
SEPTEMBER 2006

1. Purpose

The Sri Lanka Institute of Information Technology ('the Institute') has invested extensively in Information Technology ('the IT Resources') to facilitate teaching, learning, research, administration, professional development and other functions of the Institute. This Policy is intended to prescribe the appropriate behaviour and use of IT Resources by students, faculty, staff and authorised users in an effective, ethical and lawful manner. It sets out the parameters of permitted use of the IT Resources and is in addition to any other policies that govern the use of the IT Resources. In the event of a conflict between other policies and this Policy, this Policy shall prevail.

2. Scope

This Policy applies to the use of the IT Resources owned, controlled or managed by the Institute, such as computer accounts, personal computers, servers, workstations, disk storage, software, administrative and academic applications, email, public folders, newsgroups, online discussion forums, dialup, network, Internet and databases, etc. All users who have been granted access to the IT Resources ('Users'), including but not limited to the students, faculty, staff and alumni of the Institute, are to comply with this Policy. Contractors, consultants, vendors and contract workers (including their employees, agents and other authorised representatives) ('Contingent Workers') hired by a staff or faculty of the Institute ('Hiring Manager') are also to comply with this Policy.

3. Waiver

When restrictions in this Policy interfere with their research, educational or service activities, Users may request for a written waiver from specific clauses from the Head of IT Services Division. Such waiver shall only be granted in very exceptional circumstances.

4. General Prohibited Uses

4.1 Uses In Violation Of Law

Users shall not engage in any activities relating to the use of the IT Resources that will be in violation of the laws of Sri Lanka, in particular (but not limited to), the Prevention of Computer Crimes Act as may be amended from time to time. By way of illustration only, some examples of such illegal uses are:

(i) Downloading, distribution, sharing or storing of seditious, obscene or pornographic materials;

(ii) Downloading, making copies, distribution or sharing of any copyrighted materials or copyright infringing materials without prior permission from the copyright owner; and

(iii) Infringement of any copyright and intellectual property right.

4.2 Commercial Uses

Users shall not use the IT Resources for commercial purposes or to offer any commercial services to external parties, unless it is within their scope of employment with the Institute or with prior authorisation of the Institute.

4.3 Undermining System Integrity

Users must not undermine the security of the IT Resources, for example, by ‘cracking’ passwords or to modify or attempt to modify the files of other Users or software components of the IT Resources in an unauthorised manner.

4.4 Unauthorised Access Or Use

Users shall not access or attempt to access IT Resources to which they have not been given access or permit others to do so. Users shall not intercept or attempt to intercept or access data or communications not intended for them.

4.5 Tampering Of IT Resources

Users shall not tamper with the IT Resources that may potentially cause performance degradation, service instability, or compromise operation efficiency, security and fair use of resources.

4.6 Massive Search Instructions and Data Download

Users shall not indiscriminately issue search instructions and download data manually or via automated intelligent agents that may potentially consume large amount of network/Internet bandwidth and IT Resources, or which may degrade the network, system and/or database performance.

4.7 Unauthorised Disclosure or Transmission of Proprietary/Confidential Materials

Users shall not divulge any data which is proprietary and/or confidential to the Institute to any external party, unless with the prior written authorisation of the Institute.

5. Specific Uses Of IT Resources

5.1 Personal Responsibility

(i) Users shall not reveal their login, email passwords to anyone.

(ii) Users shall be responsible for maintaining the security of their passwords.

5.2 Network Connection Policy

(i) Every network connection point shall be connected to one computer only. Users shall not tamper with network points in any way, such as extending the cable to relocate the point to another room or open area temporarily or permanently, thereby blocking it from access by other Users.

(ii) Users shall not share any network addresses assigned.

5.3 Software Licence and Copyright

Users shall not use or install unlicensed software or programs. Users shall not infringe the copyright of any software available over the Institute network. As the Institute is bound by the terms of software licence agreements, the Users, as end-users, agree to comply with the terms and conditions of use as stated in the respective software licences, a copy of which is available for your perusal upon request.

5.4 Email

Email is used frequently for correspondence internally and externally.

(i) Users shall not transmit libellous, slanderous, and defamatory in nature, threatening or abusive messages or any messages that may be reasonably construed as such.

(ii) Users shall not send annoying, abusive or unwanted messages to others.

(iii) Users shall not send unsolicited mass emails within or external to the Institute, without prior approval of a Divisional Head, Director or higher authority of the Institute.

(iv) Users shall not forward messages containing general appeals or warnings like ‘virus warnings’, ‘request for help’, by mass mail or otherwise. Users should instead send these messages to the IT Services Helpdesk of the Institute for verification.

(v) Users shall not forge the identity of or impersonate another person in an email.

(vi) Users shall not knowingly transmit by email any harmful or malicious content (e.g. viruses) or any other content or material that may otherwise violate the civil and criminal laws of Sri Lanka.

(vii) Users shall not flood an individual, group or the email system with numerous or large emails.

5.5 Hiring Manager

A Hiring Manager applying for an account on behalf of a Contingent Worker to access the IT Resources as part and in the course of the Contingent Worker's work shall ensure that such use by the Contingent Worker is in compliance with this Policy.

6. Institute's Access

6.1 Conditions of Access

The Institute respects privacy and recognises its critical importance in an academic setting. As private files and data may be involved, the Institute does not, in general, intend or wish to be intrusive without prior approval.

In the following limited circumstances:

(i) For identification or diagnosis of systems or security vulnerability and problems in order to preserve the integrity of the IT Resources;

(ii) Where there are reasonable grounds to believe that a violation of law or a breach of the Institute's policies may have taken place, and such access, inspection or monitoring may produce evidence of such violation or breach; or

(iii) Where specifically allowed or required under the laws of Sri Lanka,

the Institute or its representatives may access all aspects of the IT Resources, excluding Users' owned computers.

Consistent with privacy interests of the Users, Institute access without the consent of the User will occur only with the approval of Chairman, Managing Director or their authorised delegates.

6.2 User's Assistance

The User agrees to provide all possible assistance to the Institute or its representatives in relation to the activities stated at paragraph 6.1.

6.3 Use of Security Scanning Systems

Notwithstanding paragraph 6.1, Users consent to the Institute's use of scanning programs for security purposes at system and network level for computers and systems that are connected to the Institute's network. This is to ensure that any computers or systems attached to the network will not become a launching pad for security attacks and jeopardise the IT Resources. System level scanning includes scanning for security vulnerabilities and virus detection on email attachments. Users' stored files and data are excluded from the scanning.

7. Enforcement Procedures

7.1 Complaints/Reports Of Alleged Violations

Any User who believes that the security of his/her computer account and / or password has been compromised or is aware of a violation of this Policy must report the matter to the Head of IT Services Division, who shall investigate the allegation and, if appropriate, refer the matter to the Institute disciplinary and/or law enforcement authorities.

7.2 Disciplinary Procedures

Alleged violations of this Policy will be pursued in accordance with the appropriate disciplinary procedures for students, faculty and staff.

7.3 Network Connection and Computer Account

In the event that the situation poses an immediate security threat to the IT Resources or other external systems and jeopardises the reputation, properties or other interests of the Institute, the Institute may disconnect the User’s computer or any IT equipment from the Institute’s network or disable his/her computer account for further pending actions and notify the User accordingly.

7.4 Legal Liability For Unlawful Use

In addition to disciplinary actions taken by the Institute, Users may be subject to criminal prosecution, civil liability or both for unlawful use of any of the IT Resources. Users are reminded that unauthorised access to, modification or interception of computer programmes or data can amount to serious criminal offences under the Prevention of Computer Crimes Act and the general law.

8. Channel of Recourse

Any User who suspects that the Institute or its representatives have made unwarranted access to his or her computer systems may feed back his or her concerns to the Managing Director / Chief Executive Officer, who will investigate the report.

9. Indemnity

Failure by Users to observe the abovementioned policies may result, whether directly or indirectly, in the Institute being involved in claims and/or suffering damages, losses and expenses. The User shall indemnify the Institute and its officers from any such claims, damages, losses and expenses resulting from the User's failure to observe any of the provisions of this Policy.

10. Consent To Disclosure of Information

In addition, the User must understand that the Institute will cooperate in any official investigations resulting from any breach of this Policy and may, in its discretion, furnish the relevant authorities/parties with the relevant information and your consent to any such disclosure shall be deemed by your acceptance of this Policy.

11. Changes To Policy

The Institute environment is a fast-changing environment and computer technologies and network access may be subject to change at any time. The Institute reserves the right to amend this Policy or implement additional policies, without the User's consent, from time to time in the future. Although the IT Services Division will inform Users of policy changes, Users must share the responsibility of staying informed about the Institute's policies regarding the use of IT Resources and complying with all other applicable policies. The current version of the Policy can be found at http://courseweb.sliit.lk/aup.pdf

****

SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY
IT SERVICES DIVISION

USE POLICY FOR IT RESOURCES
VERSION 1.1, SEPTEMBER 2006

UNDERTAKING

I have read, understood and accepted the Use Policy, version 1.1 set out above, including any revisions to the policy.

Signature: ______________________________

Name: ______________________________

Matriculation no./ Employee no.: ______________________________

Date: ______________________________