SRI LANKA INSTITUTE OF TOURISM & HOTEL MANAGEMENT

IT Policies & Guidelines

(Release June 2021 version 1.0)

Contents

1.0 Introduction

The Sri Lanka Institute of Tourism & Hotel Management (SLITHM) is the only Government approved premier Institute in Sri Lanka, which was established by the Government in 1964.The conversion of Ceylon Hotel School into the Sri Lanka Institute of Tourism and Hospitality Management was carried out under the 2005 Tourism Act. The Sri Lanka Institute of Tourism and Hotel Management (SLITHM) 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 Policy is being documented for fair and transparent academic purpose for use of various IT resources in the SLITHM for Students, faculty, Staff, Management and visiting Guests. Basically SLITHM IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the SLITHM on the all provincial colleges.

2.0 Purpose

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 SLITHM, 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 are also to comply with this Policy.

3.0 Waiver

When restrictions in this Policy obstruct with their research, educational or service activities, Users may request for a written waiver from specific clauses from the Head of IT approved by Director General(CEO). Such waiver shall only be granted in very exceptional circumstances.

4.0 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 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.

5.0 General Restricted Uses

5.1 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:

- Downloading, distribution, sharing or storing of seditious, obscene or pornographic materials.
- Downloading, making copies, distribution or sharing of any copyrighted materials or copyright infringing materials without prior permission from the copyright owner; and Infringement of any copyright and intellectual property right.
- SLITHM will not tolerate inappropriate materials such as pornographic, racist, defamatory or harassing files, pictures, videos or email messages that might cause offence or embarrassment. Never store, use, copy or circulate such material on the laptop and steer clear of corrupt websites.
- IT Division will be constrained to disconnect client machines where potentially damaging software is found to exist. A client machine may also be disconnected if the client's activity adversely affects the Network's performance.
- Institute network and computer resources are not to be used for personal /commercial purposes.
- Network traffic will be monitored for security and for performance reasons at IT Divison.

5.2 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.

5.3 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.

5.4 Unauthorised Access or Use

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

5.5 Interfering of IT Resources

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

5.6 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.

5.7 Unauthorised Disclosure or Transmission of Proprietary/Confidential Materials

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

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

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

6.0 Specific Use of IT Resources

6.1 IT Hardware Installation Policy

SLITHM network user community needs to observe certain precautions while getting their computers or peripherals installed so that he/she may face minimum inconvenience due to interruption of services due to hardware failures.

a) Primary User

An individual in whose room the computer is installed and is primarily used by him/her is considered to be “primary” user. If a computer has multiple users, none of whom are considered the "primary" user, the department/division Head should make an arrangement and make a person responsible for compliance.

b) End User Computer Systems

Apart from the client PCs used by the users, the institute will consider servers not directly administered by IT division, as end-user computers. If no primary user can be identified, the division must assume the responsibilities identified for end-users. Computer systems, if any, that are acting as servers which provide services to other users on the Intranet/Internet though registered with the IT division, are still considered under this policy as "end- users" computers.

6.2) Warranty & Annual Maintenance Contract

Computers purchased by any Division should preferably be with 3-year on site comprehensive warranty. After the expiry of warranty, computers would be maintained by IT division or by external Service provider on call basis. Such maintenance should inform IT division through HOD.

a) Laptop Usage

Laptop shall be the property of the SLITHM at all times and the employee will not have any right or interest in the said asset except using such asset during the employment or for such a duration as may be decided by the SLITHM. Employee must ensure that the laptop is being used only for official purposes and in the course of the rightful discharge of their duties and not for generating, transmitting, corresponding any content that is contrary to SLITHM policies.

- Assistant Lecturer/Assistant Director and above positions are entitled to receive official laptop.
- Any contract employee, consultant similar to the above mention grade must obtain Director General (CEO) prior approval for receive an official laptop.
- Minimum lifespan of an official laptop provided by SLITHM is eight (8) years and if any laptop defects before the said period, purchase of new laptop issued after inspection and recommendation by Head of IT division.
- Viruses are a major threat to the authority and laptops are particularly vulnerable if their anti- virus software is not kept up to date. The antivirus software must be updated at least monthly.
- Do not download, install or use unauthorized software programs · Any software that is required to be installed must be installed through the IT division.

7.0 Maintenance of Computer Hardware & Peripherals

IT Division is responsible for maintenance of the institute owned computer systems and peripherals that are under warranty or out of the warranty.

IT Division may receive complaints from division/users, if any of the computer or peripherals hardware related problems are noticed by them such complaints should be made by ANNEXTURE 01.

IT Division may receive complaints from the users if any of the user is not able to access network due to a network related problem at the user end. Such complaints may be generally through phone and email to IT@slithm.edu.lk.

8.0 Software Installation and Licensing Policy

Any computer purchases made by the individual divisions should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed.

8.1) Operating System and its Updating

Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through Internet. This is particularly important for all MS Windows based computers (both PCs and Servers). Updating OS by the users helps their

computers in fixing bugs and vulnerabilities in the OS that were periodically detected by the Microsoft for which it provides patches/service packs to fix them.

8.2) Antivirus Software and its updating

Computer systems used in the SLITHM should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy. Individual users should make sure that respective computer systems have current virus protection software installed and maintained. He/she should make sure that the software is running correctly. It may be noted that any antivirus software that is running on a computer, which is not updated or not renewed after its warranty period, is of practically no use. If these responsibilities appear beyond the end user's technical skills, the end-user is responsible for seeking assistance from IT Division.

8.3) Backups of Data

Individual users should perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible. IT Divison will not be liable for the loss or corruption of data on the individual user’s computer as a result of the use and/or misuse of his/her computing resources (hardware or software) by the user or from any damage that may result from the advice or actions of IT Division staff member in the process of helping the user in resolving their network/computer related problems.

9.0 Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculties, staff , and the SLITHM's managements, it is recommended to utilize the institute’s e-mail services, for formal Institute communication and for academic & other official purposes.

Email for formal communications will facilitate the delivery of messages and documents to SLITHM and extended communities or to distinct user groups and individuals. Formal Institute communications are official notices from the Institute to faculty, staff.

These communications may include administrative content, such as human resources information, policy messages, general Institute messages, official announcements, etc to receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging on to https://gmail.com with their User ID and password. For obtaining the institute’s email account, user may contact IT Divison for email account and default password by submitting an application attached Annexure 02.

Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

- Each staff member (permanent/contract basis) should have an official email address and should not communicate from personnel email accounts.
- The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.

- Using the facility for illegal/commercial purposes is a direct violation of the institute's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
- User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer; as such messages may contain viruses that have potential to damage the valuable information on your computer/Laptop.
- User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
- While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.
- Impersonating email account of others will be taken as a serious offence under the institute IT security policy.
- It is ultimately each individual's responsibility to keep their e-mail account free from violations of institute's email usage policy.

10.0 Web Site Hosting Policy

10.1 Official Pages

The IT Division is responsible for maintaining the official web site of the institute(SLITHM.EDU.LK). SLITHM official website hosted in a webserver by selected service provider and during the contract period selected service provider will maintain the website under supervision of IT Division.

10.2 Responsibilities for updating Web Pages

Divisions, faculty and individuals are responsible to send updated information time to time about any update or relevant information to Marketing Division regarding the content of the website, IT Division will support technically accordingly.

11.0 Database Use Policy

This Policy relates to the databases maintained by the institute. Data is a vital and important Institute resource for providing useful information. Its use must be protected even when the data may not be confidential. SLITHM has its own policies regarding the creation of database and access to information and a more generic policy on data access. Combined, these policies outline the institute's approach to both the access and use of this institute resource.

Here are some general policy guidelines and parameters for division and data users:

- The institute's data policies do not allow the distribution of data that is identifiable to a person outside the institute.
- Data from the Institute's Database including data collected by divisions or individual faculty and staff, is for internal institute purposes only.
- One's role and function define the data resources that will be needed to carry out one's official responsibilities/rights. Through its data access policies, the SLITHM makes information and data available based on those responsibilities/rights.
- Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the DG/CEO.
- Requests for information from any courts, attorneys, etc. are handled by the Office and divisions should never respond to requests, even with a subpoena.
- All requests from law enforcement agencies are to be forwarded to the DG/CEO for response.
- Tampering of the database by the divisions or individual user comes under violation of IT policy. Tampering includes, but not limited to:

  -Modifying/deleting the data items or software components by using illegal access methods.

  -Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ divisions.

  -Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.

  -Trying to break security of the Database servers.

Such data tampering actions by institute member or outside members will result in disciplinary action against the offender by the SLITHM authorities.

If the matter involves illegal action, law enforcement agencies may become involved.

11.1 Student Management System

Database Ownership

SLITHM Registrar office is the data owner of the entire SMS data generated in the institute.

Data Administrators

Data administration activities outlined may be delegated to some of the officers in that division.

11.2 Library Management System

Database Ownership

SLITHM Library is the data owner of the entire Library Management System data generated in the institute.

Data Administrators:

Data administration activities outlined may be delegated to some of the officers in that division.

11.3 Accounts System (QuickBooks, Payroll System)

Database Ownership

SLITHM Finance Division is the data owner of the entire Accounts System data generated in the institute.

Data Administrators

Data administration activities outlined may be delegated to some of the officers in that division.

11.4 Wifi/Network Management System

Database Ownership

SLITHM IT Divison Library is the data owner of the entire Library Management System data generated in the institute.

Data Administrators

Data administration activities outlined may be delegated to some of the officers in that division.

12.0 SLITHM Wireless Fidelity (WiFi) Policy

Usage of Wireless infrastructure in SLITHM is to enhance the accessibility of internet for academic purposes and to browse exclusive online resource of the SLITHM for student's/faculty members and staffs.

Four Service Set Identifiers (SSID's)available as follows Academic, Non-Academic, SLITHM Student and SLITHM Guest.

SSID	User Group
Academic	Faculty Staff Members
Non-Academic	Non-Academic Staff Members
SLITHM Student	Students
SLITHM Guest	Guests

- Availability of the signal will vary from place to place. The signal strength also may vary from location to location. It is not mandatory that each and every area in each floor of every block will have the same kind of signal strength, coverage and throughput.

- Access to Wireless internet is only an extended service and neither students nor anyone who is residing in the SLITHM can demand the service. Availability of wireless services solely depends on the discretion of the SLITHM and it has rights to stop/interrupt the services at any given point of time, if required for any technical purpose.
- The access points provided in SLITHM are the property of SLITHM and any damage or loss of the equipment will be considered as a serious breach of institute's code of conduct and disciplinary action will be initiated on the student/s who are found guilty for the loss or damage of the Wireless Infrastructure or the corresponding equipment in the buildings.

13.0 Internet and Web Application Filter

SLITHM-HQ and all the provincial colleges has internet connection. SLITHM-Colombo has two 100Mbps Sri Lanka Telecom PLC (SLT) fiber connection and one Dialog 4G as a backup connection.

Application	Academic	Non-Academic	Student	Guest
You tube	Allow	Allow	Deny	Deny
Facebook	Time Based	Time Based	Deny	Deny
What's App/Viber	Allow	Allow	Allow	Allow
Video Conference(Zoom/Google Meet, Teams etc)	Allow	Allow	Allow	Allow
Online Games	Deny	Deny	Deny	Deny
News Media	Allow	Allow	Allow	Allow
Software Update	Allow	Allow	Deny	Deny
Entertainment (Movie Download, torrent etc)	Deny	Deny	Deny	Deny

Time Based applications will allow during the Lunchtime from 12:30pm to 1:30pm.

13.1 Default Block Category in Firewall

- Weapon
- Phishing and fraud

- Militancy and Extremist
- Gambling
- Pro-Suicide and self-Harm
- Criminal Activity
- Marijuana
- Intellectual Piracy
- Hunting and Fishing
- Legal highs
- Controlled substances
- Anonymizers
- Sexually Explicit
- Nudity
- Peer to Peer

14.0 Video Surveillance Policy

The system has been installed by SLITHM with the primary purpose of reducing the threat of crime generally, protecting SLITHM premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy.
Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private locations or inside divisions. Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, and visitors that a CCTV Camera installation is in use.
Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

These purposes will be achieved by monitoring the system to

• Deter those having criminal intent

• Assist in the prevention and detection of crime

• Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order

• Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.

CCTV footage provided by the SLITHM IT Division upon receiving the requests from the individuals on prescribed ANNEXURE 03.

CCTV server system should locate in designated IT Server room in any SLITHM location/provincial college. CCTV monitoring is conduct from SLITHM security officers and any special monitoring window should request and approved by Director General(CEO).

15.0 Responsibilities of the Administrative Units

IT Divison needs latest information from the different Administrative Division of the SLITHM for providing network and other IT facilities to the new members of the SLITHM and for withdrawal of these facilities from those who are leaving the SLITHM, and also for keeping the web site up to date in respect of its contents.

The information that is required could be broadly of the following nature

- Information about New Appointments/Promotions.
- Information about Termination of Services.
- Information of New Enrolments.

ANNEXTURES 01

Sri Lanka Institute of Tourism and Hotel Management(SLITHM)

IT Division

IT hardware and peripheral repair form

1. Full Name : _____

2. Designation: _____

3. Division: _____

4. Mobile No : _____

5.Problem Category: Desktop - ☐ Photocopy - ☐

Laptop - ☐ Other -……

Printer - ☐

6.Information: Make (Dell, HP etc.) ……. Model Number : ……

Serial Number : …… Date Purchased: ……

7.Problem/Issue : ……..

……

……..

Date & Signature of Applicant: ……

Certified by HOD:……

……IT Division Use only……

Received by IT Division: …….

(Name and Date)

Resolved Information (In house repair, hand over to service provider, Part replacement etc)

……

Date :…….

Return Information:

Issue fixed (Yes/No) :……

Item Received (Name & Date) : ……

ANNEXTURES 02

Sri Lanka Institute of Tourism and Hotel Management(SLITHM)

IT Division

Requisition Form for E-Mail Account

1. Full Name : _____

(First Name) (Middle Name) (Last Name)

2. Designation: _____

3. Division : _____

4. Mobile No: _____

5. Existing Mail Id : _____

Date: Signature of Applicant: ……

Certified by HOD:……

……IT Division Use only……

The following email ID is created for Dr. /Mr. /Ms.

_____ on *@slithm.edu.lk*

Signature on Behalf of In Charge, ……

ANNEXTURES 03

Sri Lanka Institute of Tourism and Hotel Management(SLITHM)

IT Division

Requisition for CCTV Footage

1. Name of Applicant : _____
2. Division : _____
3. Mobile No: _____
4. Email Mail Id : _____
5. Date of Footage : _____ Time : From _____To_____
6. Camera Location : _____
7. Description : _____

Date: Signature of Applicant: ……

Approval HOD:……

……IT Divison Use only……

CCTV Footage is given to Applicant.

Signature on Behalf of In Charge,

ANNEXTURES 04

Sri Lanka Institute of Tourism and Hotel Management(SLITHM)

IT Division

CCTV Monitoring Window Information Form

1. Full Name : _____

2. Designation: _____

3. Division: _____

4.No of cameras view with floors:……..

……

……

5. DG/CEO approval :……

……IT Division Use only……

Username ……

Password ……..

Remarks ……

……

Received By :……..

Date :……..