Students Information System Policy Version 1.1

A. PURPOSE

Information technology resources at the FDI is a valuable asset and must be managed accordingly to ensure their integrity and availability and also to protect the confidentiality of data for lawful purposes. This document is intended as a high-level security policy statement for use by all FDI students.

The purpose of this policy is to ensure that the confidentiality, integrity, and availability of data and resources are protected.

B. DEFINITIONS AND SCOPE

Confidentiality refers to the privacy of personal or corporate information. This includes issues of copyright.

Integrity refers to the accuracy of data. Loss of data integrity may be evident, as when a computer disc fails, or subtle, as when a character in a file is altered.

Availability is concerned with the full functionality of a system (e.g. finance or payroll) and its components.

Within this Policy, information technology resources include information assets (e.g. databases, electronic files), software assets (e.g. applications and systems software and development tools); and physical assets (e.g. computer devices such as computer, laptop, tablet, communication/network equipment such as routers, switch, data cabinet and magnetic/optical/storage media).

Note: The Policies apply to all FDI students.

C. IT SECURITY POLICY

1.0 SECURING COMPUTER HARDWARE, PERIPHERALS AND OTHER EQUIPMENT

1.1 Damage to equipment

- *"Computer equipment should be used with care. Any deliberate damage caused to computer equipment will result in disciplinary actions as per the rules and regulations or appropriate committee setup by FDI."*

  The term 'damage' includes any unauthorized installation/use to hardware/ software or network connection/s which incurs time and/or cost in restoring the facilities to their original state.

1.2 Moving computer hardware

- *"Students are not allowed to move computer hardware and associated peripherals"*

1.3 Workplace environment

- *"Students are required to keep computer labs clean and tidy at all times. Eating, drinking and smoking are strictly prohibited."*

1.4 Incident / Accident Reporting

- *"In case a problem is witnessed, incident or accident in the computer lab (computers/printers/software/network), it should be immediately reported to the Trainer/Lecturer. Failure to report may imply your responsibility of any such accident/incident or problems."*

1.5 Mobile Communication Devices

- *"Students must deactivate their cell phones, electronic pagers or other mobiles communications devices as they may interfere with the proper operations of computer equipment and at the same time disturb class and other fellow lab users."*

1.6 Hardware Setup

- *"Computer users should under no circumstance try to modify any hardware setup, repair a faulty computer equipment, open/dismantle or disconnect either power or data cables for that matter."*

1.7 Advanced Booking of Computing Lab Facilities

- *"Students requiring computing facilities outside their normal schedule should make an advanced booking."*

1.8 Faulty reporting

- *"Faulty IT equipment or problem arising with the use of IT equipment /software/service should be reported to the trainer/lecturer, year tutor or responsible person of that section"*

2.0 CONTROLLING ACCESS TO INFORMATION AND SYSTEMS

2.1 Password

- *"All users must treat password as private and highly confidential. Passwords should never be shared with any other user."*
- *"Users shall be responsible for any operation/transaction performed under his/her officially assigned login credentials"*

2.2 Shut down of Computer

- *"Student should ensure to turn off their computer when they leave their desk after completing their work, this practice enable saving of energy and also avoid over heating of the computer device, which contribute in proper running of the device."*

2.3 Right to Examine

- *"At any time and without prior notice, management reserves the right to examine e-mail, files, directories, and other information stored on the institute's computer devices or storage devices."*

3.0 INTERNET AND E-MAIL

3.1 Internet and e-mail facilities

- *"The institute's e-mail and internet facilities should be used for educational purposes only."*

3.1.1 Internet Access

Not Allowed:

- *To visit web sites with objectionable content; pornography, gambling, warez, cracks, racist, terrorism (pirated software), hacker/hacking or other objectionable materials*

- *To download material from the internet which is offensive (sexually, racially etc.), illegal and may put security at risk.*

- *To listen and view online radio/video, download music/video other than for the use of schoolwork /submissions – proper explanation to be provided to sustain such action on query*

3.1.2 Electronic Mail (E-Mail)

- *Institute's e-mail facility should be used for educational purpose*

Not Allowed:

- *Using e-mail to send jokes, gossips, rumours , harassment etc*
- *Sending or forwarding junk or chain1 e-mails.*
- *Sending information which infringes prevailing legislations in Mauritius*
- *Responding to unsolicited e-mails or "spam"*
- *Streaming video and audio unless it is used for work-related purpose*
- *Sending e-mails using another student's official FDI e-mail account*
- *Sending confidential information to third parties without authorization.*

[1] *Chain e-mail can be identified by phrases such as "please pass this on to your friends" or similar inducements that encourage you to forward the message.

4.0 COMPLYING WITH LEGAL AND POLICY REQUIREMENT

4.1 Complying with IT legislation

- *"Computer users should be fully aware and comply to the key aspects of legislation in force in Mauritius so far as these requirements impact on their duties and include inter alia:*
    a) *Data Protection Act*
    b) *The Computer Misuse and Cybercrime Act*
    c) *Electronic Transactions Act*
    d) *Copyright Act*

4.2 Complying with Information Security Policy

- *"All computer users are required to fully comply with the institute's Information Security policies. Any information security incidents resulting from non-compliance could result in :*

    - *Withdrawal or restricted use of IT facilities.*
    - *Dismissal or expulsion of student(s) following the Institute formal disciplinary procedure.*
    - *Student bearing the costs that have arisen as a consequence of equipment misuse."*

5.0 TELEPHONE SYSTEMS

5.1 Using Telephone Systems

- *"Personal calls on the telephone systems are not allowed except in urgent or emergency situations only for which proper authorization should be requested".*

6.0 OTHER ISSUES RELATING TO INFORMATION SECURITY

6.1 Playing games on FDIs' computers

- *"Playing games on FDIs' computers is strictly prohibited."*
  The institutes' computer systems can be attacked by malicious software introduced from a PC game program.

6.2 Using computing facilities for personal use

- *"Using the institute's computers for personal / private business is prohibited."*

6.3 Software

- *"Software is protected by copyright law. Unauthorized installation/copying is a violation of Copyright Act. Anyone who uses software should understand and comply with the license requirements of the software. The institute is subject to random license audits by software vendors."*

6.4 Storage up of users' data

- *"It is the responsibility of users to ensure that backups of their data are done each time a work is done and saved in their external backup devices. FDI will not be held responsible for any loss of data."*
- *Note that the Institute computers are provisioned to flush/wipe all data saved by a user on the computer , once restarted*
- *Temporary storage space provide on computers are occasionally erased without notice to users*

6.5 Operation of services

- *"It is inappropriate to deliberately perform any act which will impair the operation of any part of the computing and networking facilities or deny access to legitimate users to any part of them. This includes but is not limited to wasting computing resources, tampering with components and settings or reducing the operational readiness of the facilities."*

- *Students are and will be monitored on their collective or individual usage of IT facilities. Uses of the systems may be intercepted, recorded, copied, audited, inspected, and disclosed to authorized institution and law enforcement personnel.*

6.6 Personal screen savers and backgrounds

- *"Users are not allowed to alter screen savers and backgrounds onto the institute computers."*

7.0 VIOLATION OF THE INTERNET USAGE POLICY

In case of violation of the Internet Usage Policy, appropriate disciplinary measures will be undertaken by FDI:

7.1 For cases not deemed to be neither criminal nature nor threatening national security, student concerned will be:

(i) Informed verbally of the matter; and/or

(ii) Be requested to abide by the Internet Usage Policy; and/or

(iii)Issued a written warning; and/or

(iv)Denied Internet access

7.2 For cases deemed to be of criminal nature or threatening national security, concerned government authorities will be given support for any related inquiries according to the law of Mauritius.

Note: This policy section may be updated as and when required without prior notice. Latest version of the document should be used. It is the responsibility of the user to keep update with the latest version available

- IT Section -
July 2014