Avinashilingam Institute for Home Science and Higher Education for Women
Coimbatore - 641 043, Tamil Nadu, India
(Deemed to be University under Category 'A' by MHRD)
Re-accredited with 'A+' Grade by NAAC
Recognised by UGC under Section 12B

IT and ICT Policy

Registrar
Avinashilingam Institute for Home Science
and Higher Education for Women
(University Estd.u/s. 3 of UGC Act.1956
Coimbatore - 641 043

Approved in 114th BOM held on 16-04-2021 - Item No.: 4.6

Table of Contents

1 Overview of IT Policies

2 About the Information Technology Policy

3 Equipment Usage Policy

4 Personal Computer (PC) Standards

5 Internet Usage Policy

6 Information Security Policy

7 Email & Chat Policy

8 Software Usage Policy

Registrar
Avinashilingam Institute for Home Science
and Higher Education for Women
(University Estd.u/s. 3 of UGC Act, 1956
Coimbatore - 641 043

1 Overview of IT Policies

Information and Communication Technologies (ICTs) is a broader term for Information Technology (IT), which refers to all communication technologies, including the internet, wireless networks, cell phones, computers, software, middleware, video-conferencing, social networking, and other media applications and services. ICT Policy is a policy put into place by the Institutions' and stakeholders' who are committed to the process of bringing digital technology to all Teaching staff, non-teaching staff and students. The ICT policy framework will help University mainly in strategic planning , change management and Learning process development .

About the Institute

- ➢ The Institution is evolving itself in its academic and administrative process so as to make them student centric and user friendly by deploying latest ICT tools. The institute has 1 Gbps internet connectivity from BSNL and additional 50 Mbps from Tikona for the Main Campus and 10+40 Mbps for Satellite campus. Both campuses has WiFi connectivity, latest software based on the department needs and video conferencing facilities. The University has also been connected on NKN on One Gbps bandwidth network.

Objectives and Scope

- ➢ To make the Institution more accessible to the present and prospective stakeholders and empowering them through enhanced access to information and quality services while improving governance through the use of ICT
- ➢ To provide conducive atmosphere for effective communication for learning and student engagement .
- ➢ To create employability for the students through ICT based educational initiatives and make them self reliant.
- ➢ Create ICT infrastructure for seamlessly connecting and integrating all ICT service providers and end users

Scope of ICT policy

This policy applies to people denoted as 'Users' in this Policy using the Institutions ICT resources including

- ✧ Students enrolled in both campus
- ✧ Permanent staff and Temporary Staff employed by the Institute
- ✧ Contractors, consultants and Suppliers
- ✧ Visitors to the Institute

S. Kousalya

Registrar,
Avinashilingam Institute for Home Science
and Higher Education for Women
(University Estd. u/s 3 of UGC Act 1956)
Coimbatore - 641 043

Guiding Principles for ICT Application

An ICT application is an ICT resource provided to a user by the Institute. The Institute's ICT related activities wil be guided by the following principles.

- Provide seamless access to teaching learning and research information to its stakeholders using ICt.
- The usage of ICT will reduce operation cost and improve teaching learning and research quality
- Use of ICT fosters transparency
- Use of ICT within the Institute to protect individual privacy as per the applicable law.
- Provide ICT tools that empower the students and enable them to be responsible for their own learning

Areas of Application

a)Research

- Challenges in the Research carries out in the institute are met by interdisciplinary teams and so the researchers depend heavily on ICT to compute analyse data and information and prepare reports for the research results .
-
- Provide data capture analysis and management of tools for both qualitative and quantitative data
- Appropriate tools to check plagiarism improves credibility of research findings
- Organize training and capacity building activities to help researchers to use latest tools for research.

b)Admissions

- Provide Online registration facility for prospective students
- Conduct of Online Entrance tests for admission to various programmes the Institute offers

c) Human Resources

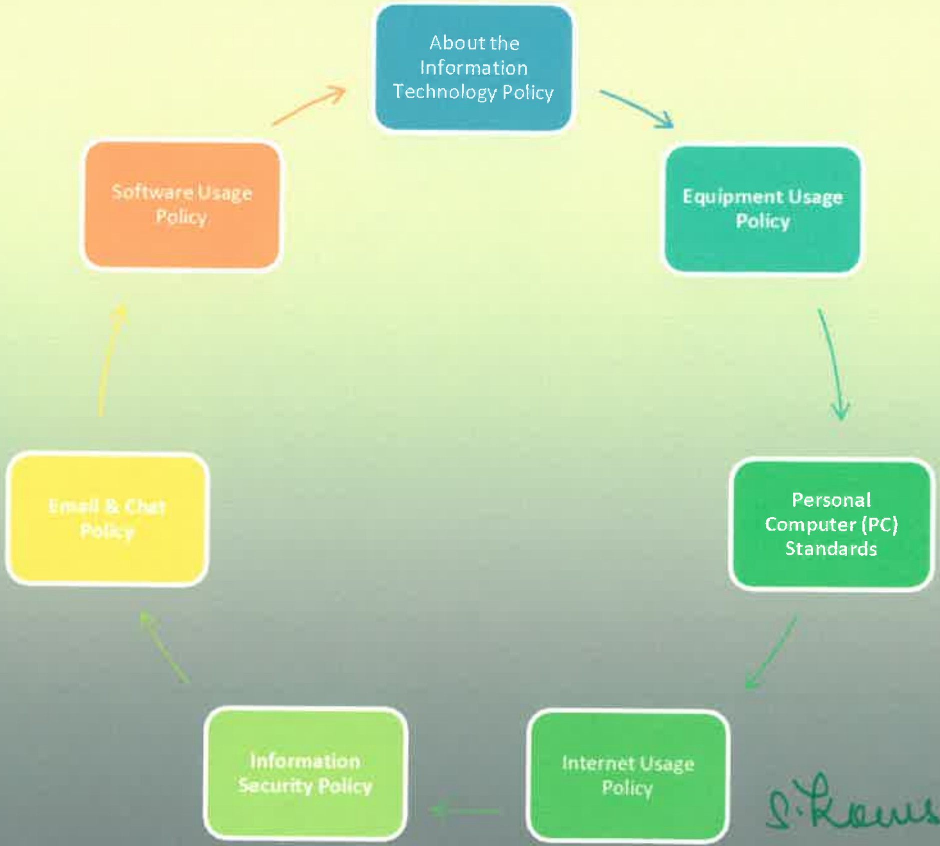
✧ ICT can be used to increase effectiveness and efficiency of the services offered by the Institute . The Institute may undertake a range of activities to support human resources through the use of ICT . Support the non-teaching staff by standardizing routine administrative activities and automating their process flow. Provide training programmes to teaching staff on latest ICT technologies

d) Teaching and Learning

- Engage teachers in selection and critical evaluation of digital content and resources (MOOCS and NPTEL etc..) to embed them Teaching–learning process
- Encourage teachers to develop e content on their own. Facilitate teachers to collaborate and undertake projects to develop high quality learning materials for students like documents ,presentations ,animations ,audio recordings and video clips
- Provide real time sessions across various institutes ,universities around the world through Webinars
- Provide training on effective use of ICT

e) Student Performance Evaluation

- Provide facilities for Online registration for examinations and share results online
- Students need to be informed about timetables and changes of the Schedule online.
- Encourage teacher to use online testing system
- Provide feedback to students on their performance on a regular basis online
- Create question bank and make it available to students



About the Information Technology Policy

Equipment Usage Policy

Personal Computer (PC) Standards

Internet Usage Policy

Information Security Policy

Email & Chat Policy

Software Usage Policy

S. Kousalya

Avinashilingam
and Higher Education for Women
(University Estd.u/s. 3 of UGC Act 1956
Coimbatore - 641 043

2 About the Information Technology Policy

2.1 Purchase

- The Procurement procedures & guidelines need to be followed to purchase new technological equipment, services or software for official purposes.
- All approved equipment, services or software will be purchased through the Computer Centre, unless informed/permitted otherwise.
- Computer Centre, plays a significant role in Procurement of items by evaluating best and most cost-effective hardware or software to be purchased for a particular dept./project/purpose based on the requirement.
- The Computer Centre, will also make sure all hardware/software standards defined in the IT Policy are enforced during such purchases.
- Complete details related to purchase of technological equipment, services or software are carried out as per UGC Guidelines.

2.2 Compliance

- All employees are expected to comply with the IT Policy rules and guidelines while purchasing, using and maintaining any equipment or software purchased or provided by the organization.
- Any employee who notices misuse or improper use of equipment or software within the organization must inform his/her Centre Manager immediately.
- Inappropriate use of equipment and software by an employee will be subject to disciplinary action as deemed by the Management Committee and Technical Committee of the organization.

2.3 Employee Training

- Basic IT training and guidance is provided to all new employees about using and maintaining their Personal Computer (PC), peripheral devices and equipment in the organization, accessing the organization network and using application software.
- Staff members both Technical and Non-technical can request the Computer Centre to conduct an IT training on a regular or requirement basis.

2.4 IT Support

- Avinashilingam Computer Centre (ACC) uses an online System to provide IT Support to its Staffs and Students.
- Students or Staff members may need hardware/software installations or may face technical issues which cannot be resolved on their own.

Registrar
Avinashilingam Institute for Home Science
and Higher Education for Women
(University Estd. u/s 3 of UGC Act 1956)
Coimbatore - 641 043

At the first level the petty problems are resolved by in-house lab assistant. In case the problem is not solved the next step is to approach the Computer Centre.

- As the next step the Lab Assistants are expected to get help from the Computer Centre for such issues via the online System or by registering Calls through Email ID only.
- Any work informed or assigned via emails sent through employee email IDs, chats or any other media except the assigned Email ID would be not entertained.
- For the sake of quick understanding, employees are expected to provide details of their issue or help required in the Ticket raised or Support Email sent.
- For major issues like PC replacement, non-working equipment, installation of application software and more, it is mandatory for all Lab in charges to inform the CC.
- For any damage to Personal Computers, approval from Computer Centre would be required for PC replacements.
- After registering calls the corresponding Laboratory Assistants should expect a solution from the CC within 1 working day. The CC staff along with Lab Assistant provide solution for the non-functionary equipment..
- Priority for solving on a First-Come-First-Served basis. However, the priority can be changed on request at the sole discretion of the designated team in Computer Centre.

3 Equipment Usage Policy

3.1 Objective

3.2Equipment Purchase

3.3 Inventory Management

Registrar
Avinashilingam Institute for Home Science
and Higher Education for Women
(University Estd.u/s. 3 of UGC Act 1956)
Coimbatore - 641 043

3.1 Objective

The Equipment Usage policy informs Laboratory in-charges and Head of the Department about equipment purchase, Department and project-level inventory management, rules for allocating & transferring equipment to employees, departments or projects and best practices for all equipment usage and maintenance.

3.2 Equipment Purchase

- ➢ The following equipments are purchased by the University with the help of Computer Centre and provided to individual departments or projects for their use. The list of equipments that can be procured are
  - ◆ Personal Computing Devices (Desktop, Laptop, Tablet)
  - ◆ Computer Peripherals (Printer, Scanner, Photocopier, Fax Machine, Keyboard, Mouse, Web Camera, Speaker, Modem etc.)
  - ◆ Networking Equipment & Supplies (Router, Switch, Wiring, etc.)
  - ◆ Biometric Devices
- ➢ The Computer Centre follows the procedures & guidelines for purchasing new equipment for official purposes. All approved equipment will be purchased through the Computer Centre, unless informed/permitted otherwise.
- ➢ The Computer Centre. will maintain a small inventory of standard PCs, software and equipment required frequently to minimize delay in fulfilling critical orders.

3.3 Inventory Management

- ➢ The Computer Centre. is responsible for maintaining an accurate inventory of all technological assets, software and tangible equipment purchased by the organization.
- ➢ The following information is to be maintained for above mentioned assets in an Inventory Sheet:
  - ◆ Item
  - ◆ Brand/ Company Name
  - ◆ Serial Number
  - ◆ Basic Configuration (e.g. HP Laptop, 120 GB HD, 2 GB RAM etc.)
  - ◆ Physical Location
  - ◆ Date of Purchase
  - ◆ Purchase Cost
  - ◆ Current Person In-Charge
- ➢ Proper information about all technological assets provided to a specific department, project centre must be regularly maintained in their respective Inventory Sheets by an assigned
- ➢ Coordinator or Stock in charge of the Department, project are to be coordinated to the centre on a regular basis. The information thus maintained about the inventory must be shared with the Computer Centre as and when

requested.

- When an Inventory Sheet is updated or modified, the previous version of the document should be retained. The date of modification should be mentioned in the sheet.
- All technological assets of the organization must be physically tagged with codes for easy identification and are to be maintained in Stock and Asset registers appropriately
- Periodic inventory audits will be carried out by the University to validate the inventory and make sure all assets are up-to-date and in proper working condition as required for maximum efficiency and productivity.

3.4 Equipment Allocation, De-allocation & Relocation

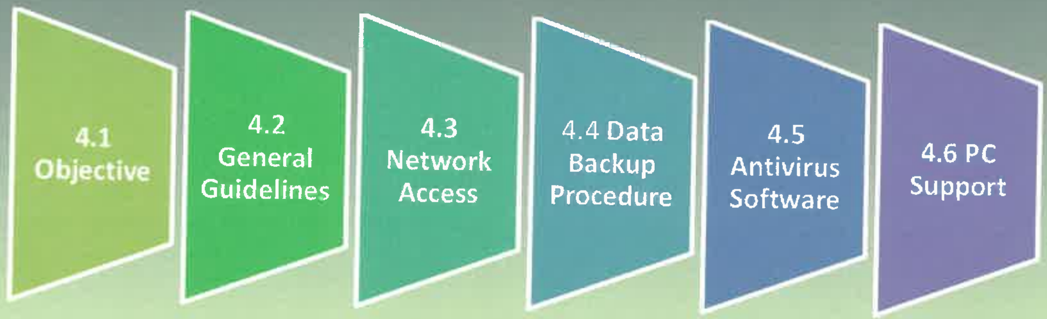
- Allocation of Assets:
- Staff members both teaching and non-teaching may be allocated a personal computer (desktop or laptop) for Department work as per work requirement.
- No employee is allowed to carry official electronic devices out of University
- De-allocation of Assets:
- It is the responsibility of the Head of the Department along with the laboratory incharges to collect all allocated organization's equipment and other assets from an employee who is leaving the organization.
- Updating the Inventory Sheet is mandatory after receiving back all allocated equipment.

3.5 Equipment Usage, Maintenance and Security

- It is the responsibility of all employees to ensure careful, safe and judicious use of the equipment & other assets allocated to and/or being used by them.
- Proper guidelines or safety information must be obtained from designated staff in the Department before operating any equipment for the first time.
- Any observed malfunction, error, fault or problem while operating any equipment owned by the organization or assigned to Staff members or Students must be immediately informed to the designated staff in Department.
- Any repeated occurrences of improper or careless use, wastage of supplies or any such offense compromising the safety or health of the equipment and people using them will be subject to disciplinary action.
- If your assigned computing device is malfunctioning or underperforming and needs to be replaced or repaired, the malfunctioning device needs to be submitted to the Computer Centre. for checking, maintenance or repair. The maintenance person will give a time estimate for repair/maintenance.

Registrar
Avinashilingam Institute for Home Science
and Higher Education for Women
(University Estd.u/s. 3 of UGC Act.1956
Coimbatore - 641 043

4 Personal Computer (PC) Standards



4.1 Objective

4.2 General Guidelines

4.3 Network Access

4.4 Data Backup Procedure

4.5 Antivirus Software

4.6 PC Support

4.1 Objective

The main aim of this policy is to maintain standard configurations of PC hardware and software purchased by the organization and provided to Staff members and Students for work. The hardware standards will help maintain optimum work productivity, computer health & security and provide timely and effective support in troubleshooting PC problems. The software standards will ensure better system administration, effective tracking of software licenses and efficient technical support.

4.2 General Guidelines

- It is the responsibility of the computer Centre to establish and maintain standard configurations of hardware and software for PCs owned by the organization. The standard, can however, be modified at any point in time as required by the Department. Head in consultation with the Senior professors.
- Multiple configurations are maintained as per the different requirements of various departments and projects in the organization, and this is procured after consultation with the Dept./Project Head.

4.3 Network Access

- All PCs being used in the University are connected to the Local Area Network as well as the Internet.
- Network security is enabled in all PCs through Firewall, Web Security and Email Security software.
- Students and Staff members are expected to undertake appropriate security measures as enlisted in the Policy.

4.4 Data Backup Procedure

S. Kousalya

Registrar
Avinashilingam Institute for Home Sc.
and Higher Education for Women
[University Estd. u/s. 3 of UGC Act 1956]
Coimbatore - 641 043

- Data Backup is setup during installation of Operating System in a PC. As an additional security measure, it is advised that Students and staff retain their assignments , Lab routine work in some external storage device also.
- File Backup System:
- Certain Department laboratories are also having a provision of server for backing up data and programs for all Student and Staff members. All Students are expected to keep their data on the file system.
- Lab incharges and Lab Assistants will have access to that data.
- Students will login to the server through the provided user ID and password.
- Server backup:
- Lab incharges and Lab Assistants are expected to maintain an incremental backup of all servers.

4.5 Antivirus Software

- Approved licensed antivirus software is installed on all PCs by theLab Assistants with the aid of Maintenance Engineers.
- Lab Assistants are expected to make sure their Antivirus is updated regularly. The Computer Centre should be informed if the Antivirus expires.
- Any external storage device like pen drive or hard disk connected to the PC needs to be completely scanned by the Antivirus software before opening it and copying files to/from the device.

4.6 PC Support

- Guidance and tips given by the Computer Centre. designated staff for maintaining the PC should be remembered while using a PC.
- The Computer Centre. should be contacted via the Email for any assistance.
- Technical support will not be provided for hardware devices or software which are personally purchased, illegal or not included in the standard hardware/software list developed by the Computer Centre.
- Software applications evaluated by the Computer Centre. to cause problems with the organization's PCs will be removed.

Registrar
Avinashilingam Institute for Home Science
and Higher Education for Women
[illegible]
Coimbatore - 641 043

5 Internet Usage Policy

5.1 Objective

The Internet Usage Policy provides guidelines for acceptable use of the organization's Internet network so as to devote Internet usage to enhance work productivity and efficiency and ensure safety and security of the Internet network, organizational data and the employees.

5.2 General Guidelines

- Internet is a paid resource and therefore shall be used only for office work.
- The organization reserves the right to monitor, examine, block or delete any/all incoming or outgoing internet connections on the organization's network.
- The organization has systems in place to monitor and record all Internet usage on the organization's network including each website visit, and each email sent or received. The Computer Centre can choose to analyze Internet usage and publicize the data at any time to assure Internet usage is as per the IT Policy.
- The organization has installed an Internet Firewall to assure safety and security of the organizational network. Any employee who attempts to disable, defeat or circumvent the Firewall will be subject to strict disciplinary action.
-

5.3 Internet Login Guidelines

- All the machines in the premises are provided with a Username and Password to login to the Internet network in the University and to monitor their individual usage.
- Staffs and Students can also get a local static IP address for

their laptops,Tablets and Mobile phones internet usage. Everybody will be responsible for the internet usage through this local static IP.

- Sharing the Username and Password with another person, visitor or guest user is prohibited.
- A visitor or guest user who wants to use the office Internet will be given a Guest Username and Password.
- The Computer Centre. will define guidelines for issuing new passwords or allowing employees to modify their own passwords.
- Any password security breach must be notified to the Computer Centre. immediately.
- Username and password allotted to an employee will be deleted upon resignation/termination/retirement from the organization.

5.4 Password Guidelines

The following password guidelines can be followed to ensure maximum password safety.

- Select a Good Password:
  - Choose a password which does not contain easily identifiable words (e.g. your username, name, phone number, house location etc.).
  - Use 8 or more characters.
  - Use at least one numeric and one special character apart from letters.
  - Combine multiple unrelated words to make a password.
- Keep your Password Safe:
  - Do not share your password with anyone.
  - Make sure no one is observing you while you enter your password so as to prevent shoulder surfing.
  - Students and Staffs are requested not write down your password in a publicly visible area.
  - Change your password periodically (every 3 months is recommended).
  - Do not reuse old passwords. If that is difficult, do not repeat the last 5 passwords.
- **Other Security Measures:**
  - Ensure your computer is reasonably secure in your absence.
  - Lock your monitor screen, log out or turn off your computer when not at desk.

5.5 Online Content Usage Guidelines

- Staffs and students are solely responsible for the content accessed and downloaded using Internet facility in the office. If they accidentally connect to a website containing material prohibited by the organization, they should disconnect from that site immediately.

- During working hours, Staffs and students are expected to spend limited time to access news, social media and other websites online, unless explicitly required for office work.
- Staffs and students are not allowed to use Internet for non-official purposes using the Internet facility in office.

5.6 Inappropriate Use

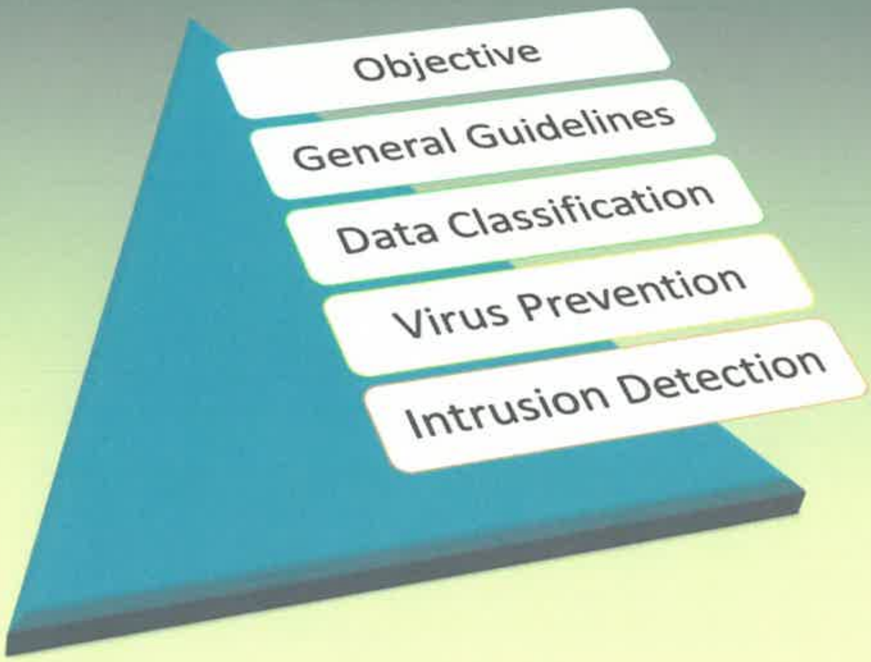
The following activities are prohibited on organization's Internet network. This list can be modified/updated anytime by the Computer Centre as deemed fit.

- Any disciplinary action considered appropriate by the Special Technical Committee (including legal action or termination) can be taken against Student involved in the activities mentioned below:
- Playing online games, downloading and/or watching games, videos or entertainment software or engaging in any online activity which compromises the network speed and consumes unnecessary Internet bandwidth
- Downloading images, videos and documents unless required to official work
- Accessing, displaying, uploading, downloading, storing, recording or distributing any kind of pornographic or sexually explicit material is prohibited
- Accessing pirated software, tools or data using the official network or systems
- Uploading or distributing software, documents or any other material owned by the organization online without the explicit permission of the Technical Committee
- Engaging in any criminal or illegal activity or violating law
- Invading privacy of co workers
- Using the Internet for personal financial gain or for conducting personal business
- Deliberately engaging in an online activity which hampers the safety & security of the data, equipment and people involved.
- Carrying out any objectionable, frivolous or illegal activity on the Internet that shall damage the organization's reputation

Registrar
Avinashilingam Institute for Home Science
and Higher Education for Women
(University Estd.u/s. 3 of UGC Act 1956
Coimbatore - 641 043

S. Kousalya

6 Information Security Policy



6.1 Objective

Information security means protection of the organization's data, applications, networks and computer systems from unauthorized access, alteration and destruction. The Information Security Policy provides guidelines to protect data integrity based on data classification and secure the organization's information systems.

6.2 General Guidelines

- Various methods like access control, authentication, monitoring and review will be used to ensure data security in the organization.
- Security reviews of servers, firewalls, routers and monitoring systems must be conducted on a regular basis. These reviews should include monitoring of access logs and intrusion detection software logs.
- Appropriate training must be provided to data users, and network & system administrators to ensure data security.

Registrar
Avinashilingam Institute for Home Science
and Higher Education for Women
(University Estd.u/s. 3 of UGC Act.1956
Coimbatore - 641 043

6.3 Data Classification

The organization classifies data into three categories:

- High Risk:
  - It includes information assets which have legal requirements for disclosure and financial penalties imposed for disclosure.
  - E.g. Students Mark List, Payroll, Personnel, financial, biometric data
- Medium Risk:
  - It includes confidential data which would not impose losses on the organization if disclosed, but is also not publicly available.
  - E.g. Timetable, Notes of Lesson, Agreement documents, unpublished reports, etc.
- Low Risk:
  - It includes information that can be freely disseminated.
  - E.g. brochures, published reports, other printed material etc.
  - Different protection strategies must be developed for the above three data categories. Information about the same must be disseminated appropriately to all relevant departments and staff.
- High risk data must be encrypted when transmitted over insecure channels.
- All data must be backed up on a regular basis as per the rules defined by the Computer Centre. at that time.

6.4 Access Control

- Access to the network, servers and systems in the organization will be achieved by individual logins and will require authentication. Authentication includes the use of passwords, biometrics or other recognized forms of authentication.
- All users of systems which contain high or medium risk data must have a strong password as defined in the IT Policy.
- Default passwords on all systems must be changed after installation.
- Where possible and financially feasible, more than one person must have full rights to any organization-owned server storing or transmitting high risk and medium risk data.

6.5 Virus Prevention

- Virus prevention for personal computers and email usage has been described previously.

S. Kousalya

- Apart from that, all servers and workstations that connect to the network must be protected with licensed anti-virus software recommended by the vendor. The software must be kept up-to-date.
- Whenever feasible, system/network administrators must inform users when a virus/ other vulnerability has been detected in the network or systems.

6.6 Intrusion Detection

- Intrusion detection must be implemented on all servers and workstations containing high
- Operating system and application software logging process must be enabled on all systems.
- Server, firewall and critical system logs must be reviewed frequently.

7 Email & Chat Policy

- 7.1 Objective
- 7.2 General Guidelines
- 7.3 Ownership
- 7.4 Confidentiality
- 7.5 Email Security
- 7.6 Inappropriate Use

7.1 Objective

This policy provides information about acceptable usage, ownership, confidentiality and security while using electronic messaging systems and chat platforms provided or approved by the organization. The policy applies to all electronic messages sent or received via the above mentioned messaging systems and chat platforms by all official employees of the organization.

7.2 General Guidelines

- The organization reserves the right to approve or disapprove which

Registrar
Avinashilingam Institute for Home Science
and Higher Education for Women
(University Estd.u/s. 3 of UGC Act.1956
Coimbatore - 641 043

electronic messaging systems and chat platforms would be used for official purposes. It is strictly advised to use the pre-approved messaging systems and platforms for official puposes

- ➢ Staffs upon joining the organization, are provided with an official email address should use it for official purposes only.
- ➢ Any email security breach must be notified to the Computer Centre. immediately.
- ➢ Upon termination, resignation or retirement from the organization, the organization will deny all access to electronic messaging platforms owned/provided by the organization.
- ➢ All messages composed and/or sent using the pre-approved messaging systems and platforms need to comply with the organization policies of acceptable communication.
- ➢ Electronic mails and messages should be sent after careful consideration since they are inadequate in conveying the mood and context of the situation or sender and might be interpreted wrongly.
- ➢ All email signatures must have appropriate designations of employees and must be in the format approved by the Technical Committee.

7.3 Ownership

- ➢ The official electronic messaging system used by the organization is the property of the organization and not the employee. All emails, chats and electronic messages stored, composed, sent and received by any employee or non-employee in the official electronic messaging systems are the property of the organization.
- ➢ The organization reserves the right to intercept, monitor, read and disclose any messages stored, composed, sent or received using the official electronic messaging systems.
- ➢ The organization reserves the right to alter, modify, re-route or block messages as deemed appropriate.
- ➢ IT Administrator can change the email system password and monitor email usage of any employee for security purposes.

7.4 Confidentiality

- ➢ Proprietary, confidential and sensitive information about the organization or its employees should not be exchanged via electronic messaging systems unless pre-approved by the Reporting Manager(s) and/or the Management Committee.
- ➢ Caution and proper judgment should be used to decide whether to deliver a message in person, on phone or via email/electronic messaging systems.
- ➢ Before composing or sending any message, it should be noted that electronic messages can be used as evidence in a court of law.
- ➢ Unauthorized copying and distributing of copyrighted content of the

Registrar
Avinashilingam Institute for Home Science
and Higher Education for Women
[illegible]
Coimbatore - 641 043

organization is prohibited.

7.5 Email Security

Anti-Virus:

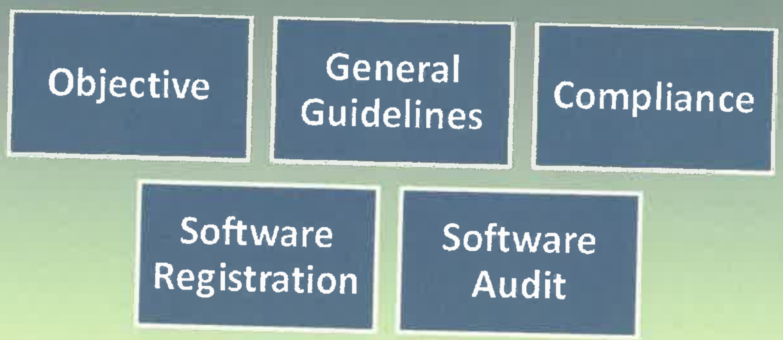
- Anti-virus software pre-approved by the Dept. Head - IT should be installed in the laptop/desktop provided to a new employee after joining the organization.
- All employees in the organization are expected to make sure they have anti-virus software installed in their laptops/desktops (personal or official) used for office work.
- Organization will bear responsibility for providing, installing, updating and maintaining records for one anti-virus per employee at a time for the official laptop provided by the organization. The employee is responsible for installing good quality anti-virus software in their personal laptop/desktop used for office work.
- Employees are prohibited from disabling the anti-virus software on organization- provided laptops/desktops.
- Employees should make sure their anti-virus is regularly updated and not out of date.
- **Safe Email Usage:** Following precautions must be taken to maintain email security:
- Do not to open emails and/or attachments from unknown or suspicious sources unless anticipated by you.
- In case of doubts about emails/ attachments from known senders, confirm from them about the legitimacy of the email/attachment.
- Use Email spam filters to filter out spam emails.

7.6 Inappropriate Use

- Official Email platforms or electronic messaging systems including but not limited to chat platforms and instant messaging systems should not be used to send messages containing pornographic, defamatory, derogatory, sexual, racist, harassing or offensive material.
- Official Email platforms or electronic messaging systems should not be used for personal work, personal gain or the promotion or publication of one's religious, social or political views.
- Spam/ bulk/junk messages should not be forwarded or sent to anyone from the official email ID unless for an officially approved purpose.

Registrar
Avinashilingam Institute for Home Science
and Higher Education for Women
(University Estd.u/s. 3 of UGC Act.1956
Coimbatore - 641 043

8 Software Usage Policy


Objective

General Guidelines

Compliance

Software Registration

Software Audit

8.1 Objective

The Software Usage Policy is defined to provide guidelines for appropriate installation, usage and maintenance of software products installed in organization-owned computers.

8.2 General Guidelines

- Third-party software (free as well as purchased) required for day-to-day work will be pre- installed onto before handing over to Students and Staffs. A designated person in the Computer Centre. can be contacted to add to/delete from the list of pre-installed software on organizational computers.
- No other third-party software – free or licensed can be installed onto a computer system owned or provided to Staff member by the organization, without prior approval of the Computer Centre.
- To request installation of software onto a personal computing device, Aid of Lab Assistants can be sought.
- Any software developed & copyrighted by the organization belongs to the organization. Any unauthorized use, storage, duplication or distribution of such software is illegal and subject to strict disciplinary action.
-

8.3 Compliance

- No employee is allowed to install pirated software on official computing systems.
- Software purchased by the organization or installed on organizational computer systems must be used within the terms of its license agreement.
- Any duplication, illegal reproduction or unauthorized creation, use and distribution of licensed software within or outside the organization is strictly

S. Kousalya

prohibited. Any such act will be subject to strict disciplinary action.

- Any employee who notices misuse or improper use of software within the organization must inform his/her Reporting Manager(s).

8.4 Software Registration

- Software licensed or purchased by the organization must be registered in the name of the Registrar/organization with the Job Role or Department in which it will be used and not in the name of an individual.
- After proper registration, the software may be installed as per the Software Usage Policy of the organization. A copy of all license agreements must be maintained by the Computer Centre.
- After installation, all original installation media (CDs, DVDs, etc.) must be safely stored in a designated location by the Computer Centre.

8.5 Software Audit

- The Computer Centre. will conduct periodic audit of software installed in all company-owned systems to make sure all compliance are being met.
- Prior notice may or may not be provided by the Computer Centre. before conducting the Software Audit.
- During this audit, the Computer Centre. will also make sure the anti-virus is updated, the system is scanned and cleaned and the computer is free of garbage data, viruses, worms or other harmful programmatic codes.
- The full cooperation of all employees is required during such audit

Reviewed and Modified On :10/03/2021
Next Review Date : 31/03/2024

S. Kousalya

Registrar
Avinashilingam Institute for Home Science
and Higher Education for Women
(University Estd.u/s 3 of UGC Act 1956)
Coimbatore - 641 043