# Amrita Vishwa Vidyapeetham

## Information and Communication Technology Services Department

## Information Technology (IT) Policy

### 1. General statement

1.1 Information and Communication Technology Services (ICTS) Department at Amrita Vishwa Vidyapeetham aims at identifying, providing and maintaining reliable computing facilities, computing network environment, communication facilities and related infrastructure to facilitate education, research, instructional and Institute approved business services.

1.2 ICTS shall try to use the best available technical solutions to fulfill the objectives mentioned in Para 1.1.

1.3 ICTS reserves the right to monitor the usage of the facilities provided therein to maintain a secure computing environment and to abide by the legal norms that exist.

1.4 In this document, the term "users" shall mean individuals, staff, students, departments, offices, institutes, schools or any other entity which fall under the management of Amrita Vishwa Vidyapeetham, Ettimadai campus and require any services aforesaid.

1.5 This document is meant for internal circulation and all users shall have access to this document.

1.6 Students shall also be bound by all the rules and regulations formulated by the University from time to time on use of computing facilities provided to them or owned by them.

1.7 User groups shall identify one member from their group to coordinate all ICT related matters with ICTS.

### 2. General responsibilities of users

2.1 All users shall comply to existing federal, state and other applicable laws.

2.2 Honoring acceptable use policy of networks accessed through Amrita Vishwa Vidyapeetham's campus network.

2.3 Abiding by existing telecommunications and networking laws and regulations.

2.4 Following copyright laws regarding protected commercial software or intellectual property.

2.5 Minimizing unnecessary network traffic that may interfere with the ability of others to make effective use of campus network resources.

2.6 Not overloading networks with excessive data or wasting the University's other technical resources.

## 3. Acceptable devices

3.1 Any computer, peripheral or network capable device connected to campus network must belong to, or be formally registered, or be hosted by ICTS.

3.2 ICTS reserves the right to restrict access otherwise.

## 4. Computing facility provision and maintenance.

4.1 ICTS is responsible for provision and maintenance of computing facilities provided to users. The facilities are provided after the user secure approvals from competent members of administration.

4.2 The facility assigned to the user shall be used for purposes as mentioned in Para 1.1.

4.3 The user shall ensure physical safety of the equipment and produce the same as and when required for stock verification by ICTS. If any peripheral or components of the equipment assigned is found missing, the user shall report the same to ICTS for further action.

4.4 The user shall obtain prior approval from ICTS before plugging in any additional peripherals to the equipments internally. The user may use external peripherals connected via existing external ports available on the equipment (USB, RS232, IEEE1394, etc.).

4.5 ICTS shall not be responsible for any failure to personal peripherals connected to university equipment by the user.

4.6 Users shall ensure data security by taking regular backups of the data stored on their systems.

4.7 The individual or the department shall be responsible to report any hardware or software related faults to ICTS through facilities provided for reporting. ICTS shall take all necessary steps to resolve the issue at the earliest. However, faults that require substantial additional financial expense may need to be approved by competent authorities.

4.8 All support calls attended by support personnel shall be documented and the user or department shall insist to get a written service report from the service personnel regarding the support offered. The individual or the department shall ensure that the service report is complete in all respect including components that have been removed or replaced by the service personnel.

4.9 The ownership of the equipment assigned to the individual or the department shall remain with the University.

4.10 Possession of computing equipments by students within the campus shall be governed by the rules and regulations formulated by the University separately. However, students shall be bound by all the provisions of the IT policy with respect to the usage of such equipments with the campus.

## 5. Provision of computing software and maintenance

5.1 ICTS shall provide all necessary software for operating the devices allocated to the user.

5.2 ICTS reserves the right to secure the administrative passwords for all the devices owned by the University.

5.3 Users may install any software on the equipments allotted to them after obtaining prior approval from ICTS. All such software that may be installed on the equipment shall be used for the purposes as mentioned in Para 1.1. However, ICTS shall reserve the right to restrict users from installing any software that may pose a risk to the security and integrity of the equipment and the campus network.

5.4 All software installed on the user machines shall be legal copies from the original vendors. Users are encouraged not to use any illegal or unlicensed versions of copyrighted software.

5.5 ICTS shall ensure reinstallation of system and application software if required. Users shall request for the same through facilities provided for making such support requests.

5.6 Users shall not copy, duplicate or distribute any software owned by the University or downloaded by them to their PCs.

## 6. Provision of network connectivity and maintenance

6.1 ICTS is responsible for providing users with data communications connectivity from their building to all campus-wide network services.

6.2 ICTS provides data communications connectivity to allow access from a terminal, PC, accepted devices or user group to campus-wide network services for purposes mentioned in Para 1.1.

6.3 ICTS is responsible for the design, development, and maintenance of campus-wide network facilities that are used to connect all users, including facilities such as ISDN, leased data links, fiber optic backbone network or any other technologies that may be adopted.

6.4 ICTS will test and monitor the shared networks to detect problems, and will take actions necessary to isolate the cause and correct the problem.

6.5 Personal devices of users shall be connected to the network after registering the same with the ICTS.

## 7. User group data network responsibilities

7.1 Individual departments, users or user groups may develop their own local area networks or local communications environment within, only if those facilities are approved by ICTS and meets developed network standards. ICTS shall also reserve the rights to monitor such networks.

7.2 Any user group or department intending to establish connectivity to external data communications network directly should do so after coordinating with ICTS. ICTS shall extend all necessary technical support to user groups or departments who intend to establish such connections to external data communications. All such direct communication networks shall be routed physically or

logically through the central network operations centre of ICTS to maintain security to the campus network.

## 8. Campus network security

8.1 Computer networks are designed to be open systems and facilitate access to networked resources, data applications system security must rely primarily on the proper application system design and network operating system configuration, rather than on secure physical network facilities.

8.2 ICTS is responsible for maintaining physical security of all network equipment and data communications cabling in campus equipment closets, between buildings and in network hub locations..

8.3 ICTS is responsible for the integrity of all software running on the backbone network equipment, including network control servers, communications servers, bridges, routers, and gateways.

8.4 Users are encouraged to assist ICTS in maintaining the physical security of the network assets installed at their location and also to ensure the integrity of all network related services running on their local hosts.

8.5 ICTS shall take all necessary security measures to protect and secure the device connected to network and avoid compromises. This may include undisclosed administrator level passwords, restricted access to external or internal ports, restriction on installation of system software by the users, etc.

8.6 Compromised or problem hosts connected to the network, once identified will be blocked until they are repaired.

8.7 To ensure network security, ICTS shall monitor all traffic on the network using appropriate software to identify malicious traffic. If malicious traffic is identified, the host that generated or generating the traffic shall be logically or physically disconnected from the network. ICTS shall recommend remedial actions for such devices connected to the network, which may include: removal of malicious software, fully patched Operating Systems; current anti-virus software and virus definitions; secure passwords, personal firewalls, intrusion detection software, etc. ICTS shall provide necessary support to users for the aforesaid actions.

8.8 ICTS shall implement necessary mechanisms to ensure physical security of equipments installed in the campus. This may include but not limited to installation of audio and or video supported surveillance equipments.

8.9 ICTS shall also extend support to users connecting their personal devices to the campus network, but limited to the operational or legal constraints.

## 9. Provision of network services

9.1 ICTS shall host all necessary network services to support the activities of the users. This shall include internet connectivity, email services, ftp servers, DNS, DHCP, etc. The usage of the services shall be for the purposes as mentioned in Para 1.1 and shall be monitored and controlled by ICTS.

9.2 These services are provided for the purpose of increasing the job fulfillment, job performance, and to increase the productivity.

9.3 Users shall fill up necessary application forms to access services hosted by ICTS.

9.4 Some of the services shall be available to users by default on the network, which includes access to intranet services, digital library access, learning management services servers, etc.

9.5 Users shall not divulge passwords, software license codes or other security codes allotted to them to third party. Users are encouraged to reset their passwords every 60 days to ensure access security.

9.6 Users shall not use Amrita Vishwa Vidyapeetham network services to view, download, save, receive or send material related to or including :

9.6.1 Offensive content of any kind, including pornographic material

9.6.2 Promoting discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion or disability.

9.6.3 Threatening or violent behavior.

9.6.4 Illegal activities.

9.6.5 Commercial messages.

9.6.6 Messages of a political or racial nature.

9.6.7 Gambling.

9.6.8 Sports, entertainment, and job information and/or sites.

9.6.9 Personal financial gain.

9.6.10 Forwarding e-mail chain letters.

9.6.11 Spamming e-mail accounts from Amrita Vishwa Vidyapeetham's e-mail services or computers.

9.6.12 Material protected under copyright laws.

9.6.13 Sending business-sensitive information by e-mail or over the Internet.

9.6.14 Dispersing organizational data to non-Amrita personnel without authorization.

9.6.15 Opening files received from the Internet without performing a virus scan.

9.6.16 Recreational streaming of internet material, such as radio, video, TV, or stock tickers.

9.6.17 Downloading and/or installing programs/software on any network computer(s) without authorization from the IT Services Department.

9.6.18 Tampering with your Amrita domain e-mail ID in order to misrepresent yourself and Amrita to others.

9.7 ICTS may shutdown the network services periodically for maintenance purposes. Users shall be informed well in advance regarding such outages.

9.8 Information regarding such maintenance schedules shall be sent to users through available means of communication which may include but not limited to emails, web announcements or hard copy circulars.

## 10. Network activities not allowed over the campus network

10.1 Execution of software programs which excessively consume network or network server resources

10.2 Activities that violate local administration, state, central government or recognized international organization or treaties.

10.3 Activities that interfere with the legitimate function of other devices connected to campus network. (examples include DHCP Servers, devices running RIP, RAS Servers consuming DHCP Addresses which have not been registered with ITES, etc.)

10.4 Configuring mail servers with open relays, sending unsolicited mails, commercial mails, spamming.

10.5 Downloading large files for personal use including music, video and software.

10.6 Initiating Denial of Service Attacks, Hacking, Cracking or similar activities which disrupt the network services hosted internally and externally

10.7 Probing, scanning or other activities that amount enumeration of campus network.

10.8 Executing network related software for packet sniffing, content sniffing.

10.9 Unauthorized access to internal or external network services, servers or hosts.

10.10 Illegal distribution of any copyrighted material

10.11 "Stealing" or "Borrowing" IP addresses

10.12 Visiting websites that do not come under the purview of objectives mentioned in Para 1.1

10.13 Any activity that tarnishes Amrita Vishwa Vidyapeetham's professional image. (ICTS may not be the policing agency in these matters)

## 11. Violations

11.1 Violations will be reviewed on a case-by-case basis.

11.2 If it is determined that a user has violated one or more of the above use regulations, that user will receive a reprimand from his or her Head of the Department or

reporting authority and his or her future use will be closely monitored.

11.3 If a gross violation has occurred, management will take immediate action. Such action may result in losing Internet and/or e-mail privileges, severe reprimand, and or disciplinary action.

11.4 During the investigation of an alleged policy violation, a user's computing and network access may be suspended.

11.5 The decision of the management shall be final and binding on the constituents in case of any conflict or dispute.

## 12. Revision

12.1 Proposed revisions of this policy should be reviewed by a committee which shall include :

Pro-Chancellor

Vice Chancellor

Dean - Engineering

Registrar

Head – ICTS

Two external experts

Updated : 18th August, 2015