



**DAYANANDA SAGAR UNIVERSITY**

**APPROVED**

**IT POLICY**

**VERSION 3.1**

**19<sup>TH</sup> SEPTEMBER 2022**

**Change History:**

Sl. No.	Date	Section No	Change Description	Reason for change	Section Revision No.	Current Document Version Number
1	04 Oct 2022	1,2,3	Introduction, scope and Objectives included	To bring more clarity		1.1

**Date of Release by IT MANAGER: 20 January 2020**

Prepared By	Reviewed by	Approved By
Dr. Kiran B Malagi Dr. Girisha G S Mr. Sukumar Reddy T	Dr. Udaya Kumar Reddy K R Dean, SoE	Dr. Puttamadappa C Registrar
<b>31 Aug 2022</b>	<b>10 September 2022</b>	<b>19 September 2022</b>



## **INTRODUCTION**

Dayananda Sagar University, Bangalore (DSU), encourage IT Support in education, instructional, research and all administration activities in order to enhance the productivity. The policy document specifies the IT resources procurement, usage and decommissioning of the same.

## **SCOPE**

The policies process applies to all the users of computational resource owned and managed by Dayananda Sagar University. The users are, Dayananda Sagar University faculty (Regular / Visiting / Adjunct / Emeritus), staff members, students, guest, alumni originations departments, offices, affiliates school and any other entities accessing the networking / computational services of Dayananda Sagar University.

## **OBJECTIVES**

- a. This main objective of this policy is to maintain, secure, and ensures authorized / legal usage of IT infrastructure.
- b. The Polices provides strategies and responsible for ensuring confidentiality, integrity and availability of the information of assets of the university.

The IT Department of Dayananda Sagar University is running the Firewall security, Proxy, DHCP, DNS, email, web and application servers and manage the network of the college. It has been taking appropriate steps by installing firewalls, access controls and installing virus checking and content filtering software at the gateway.

## **BUDGETING ALLOCATION & EXPANSION PLANS:**

Every financial year, a budgetary allocation is prepared by the IT manager, summarized by the office of CFO and is approved by the BOG, on recommendation from BOM. The budgetary allocation involves, new acquisitions, planned and already approved, maintenance and future expansions to the year.



## **CLASSIFICATION OF IT POLICIES**

### **1.1 IT Hardware Installation Policy**

The network user community of the college needs to observe certain precautions while getting their computers or peripherals installed so that they may face minimum inconvenience due to interruption of services due to hardware failures.

Computers purchased by any Section/Department/Project should preferably be with 3-year on-site comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include OS reinstallation and checking virus related problems. Department HODs should monitor for the proper and timely maintenance of IT hardware.

### **1.2 Software Installation and Licensing Policy**

DSU encourages all members of its community to use Free and Open-Source Software (FOSS)

Any computer purchases made by the individual, departments, and cells should make sure that such computer systems have all licensed software like operating system, antivirus software and necessary application software etc. installed. Institute IT policy does not allow any pirated software installation on the institute owned computers and the computers connected to the institute campus network. In case of any such instances, institute will hold the department/individual personally responsible for any pirated software installed on the computers located in their department rooms.

Individual users should make sure that respective computer systems have current virus protection software installed and maintained.



### 1.3 ROLES & RESPONSIBILITY

- a) DSU shall set up an IT department in the University and implement appropriate controls to ensure compliance with this policy by their users.
- b) Procurement of any IT infrastructure will be as per the DSU norms.
- c) IT department shall ensure resolution of all incidents related to the security aspects of this policy by their users. Necessary support can be obtained from the Implementing Agency.
- d) The IT resources are to be utilized only for the activities that are consistent with the academic, research and public service mission of the University and are not "Prohibited Activities.
- e) All users shall comply to existing national, state and other applicable laws.
- f) Abide by existing telecommunications and networking laws and regulations.
- g) Follow copyright laws regarding protected commercial software or intellectual property. DSU provides access to scholarly and/or work-related tools, including access to the Library, certain computer systems, and servers, software and databases and the Internet to its members. It is expected that unobstructed use of these tools, of certain degrees of privacy and of protection from abuse and intrusion by others sharing these resources.
- h) Authorized users can expect their right to access information and to express their opinion to be protected as it is for paper and other forms of no electronic communication.
- i) Users shall not install/uninstall any network/security device. Any such requirement will be brought to the notice off the IT team and further actions will be taken up by the team.
- j) The timely updates in the policy will be brought to the notice of the users and it is expected that the users will be abide by such rules.



## **1.4 PRIVACY & PERSONAL RIGHTS**

- Usage / access to the email, data, and program are other files without the concern or approval from the competent authority is not allowed.
- Usually there will be no monitoring or limiting the information transmitted on the campus wide local area network (LAN), however the IT department reserves the right to access and review transmitted information during creative session with the due approval of the committee authority.

## **1.5 ACCESSING WIRELESS NETWORK**

For accessing the wireless network the user has to

- Register the devices and option the login credentials.
- Users should not connect their devices to unsecured wireless network.

## **1.6 FILTERING AND BLOCKING OF SITES**

The Connects accessed through the internet may be blocked which are in contravention of the provisions of the IT act 2000 and other applicable laws or which may post a security to the network.

The IT department (In the connection of university) may block in appropriate or any connect which may haven a negative impact on the property the user.

## **1.6 SECURITY INCIDENT MANAGEMENT**

- Any security threat that can impact the availability, integrity, confraternity and authority of the university data is considered as security incident.
- Any such device can be de active or removed from the network under intermission to the computed authority of the university
- Any Security threat notice to be brought immediately to Indian computer emergence responses team (ICERT)
- All the supporting logs shall we maintained and produced as and when its necessary.



## 1.7 E-MAIL ACCOUNT CREATION AND USE POLICY

- In order to create the mail id for the newly joined. The concerned department for which the new faculty has joined has to give requests through the mail.
- The IT department will create the login credentials and communicate the same to the concerned department. The faculty will be receiving the new login id credentials from the departments

## 1.8 EMAIL ID USAGE

- DSU provides official email access privileges to its users. In an effort to handle the efficient information dissemination among the administration, faculty members, staffs and students, it is recommended to avail official email with DSU.edu.in domain.
- Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:
- 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 university'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.
- While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.
- User should keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox almost full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
- 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 in 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.

- User should not share his/her email account's credentials with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.

### **1.9 WEB SITE HOSTING POLICY**

As on date, the college webmaster is responsible for maintaining the official web site of the college viz., *http://www.dsu.edu.in only.*

### **1.10 COLLEGE DATABASE USE POLICY**

This Policy relates to the databases maintained by the college administration under the college's e-Governance. Data is a vital and important resource for providing useful information. Its use must be protected even when the data may not be confidential.

*Sulth Ali 19/9/22*

