DAYANANDA SAGAR UNIVERSITY

IT Policy Document

Version : 1.0
Published Date : August 2024

Document Version History:

Version no	Release Date	Amendment	Author
1.0	August 2024	Initial release	Office of the CIO

Table of Contents

1. **Introduction**

This document is the official IT Security Policy Statement of Dayananda Sagar University (DSU). As an institution, DSU acknowledges the criticality of its information assets and the technological infrastructure supporting its operations. It is recognized that these assets are susceptible to various threats, including but not limited to:

a. Physical security,
b. Operations security,
c. Communications security,
d. Network security, and
e. Information security.

DSU acknowledges that adverse events stemming from these threats may result in the compromise, damage, or loss of information resources, leading to disruptions in University activities and potential breaches of confidentiality and privacy concerning information pertinent to DSU's staff and students.

In response to these risks, DSU has meticulously formulated IT Security policies designed to mitigate vulnerabilities in electronic information resources. These policies aim to implement controls capable of identifying and preventing errors or irregularities that may arise in the course of operations.

It is understood that achieving absolute security for IT resources against all conceivable threats is impractical and would necessitate an unreasonable allocation of resources. Consequently, DSU is committed to implementing robust security measures while acknowledging the inherent limitations in attaining absolute security.

This Policy Statement is legally binding and serves as a foundational document for all IT security-related initiatives undertaken by DSU. It is subject to periodic review and may be amended or supplemented as deemed necessary to ensure compliance with evolving regulatory requirements and best practices in information security.

This version emphasizes the legal significance of the IT Security Policy Statement, outlines DSU's commitment to safeguarding information assets, and highlights the acknowledgment of inherent limitations in achieving absolute security. This Policy describes the high-level direction for information security management within DSU and custodians of DSU IT assets. It is based on three concepts:

A. Confidentiality,
B. Integrity, and
C. Availability

Confidentiality ensures that DSU Information is not disclosed to anyone who is not authorized to access it.
Integrity ensures that DSU Information is correct or accurate to the degree anticipated by those who use it.
Availability ensures that DSU Information is accessible when and where it is needed.

These Policies apply to all DSU Students & Staff, and to all entities/affiliates of DSU. Implementation of these guidelines, including development of more specific standards or guidelines as needed, is the responsibility of respective stake holders and the CIO office.

The Office of the CIO under the leadership of the Vice Chancellor will work towards the implementation of this policy. The DSU Information Security policy & practices will be reviewed and evaluated once in 12 months for updates. As DSU is in the fore front of education and research, it is essential that all staff & students understand the value of DSU Information and their individual and collective responsibility to protect it.

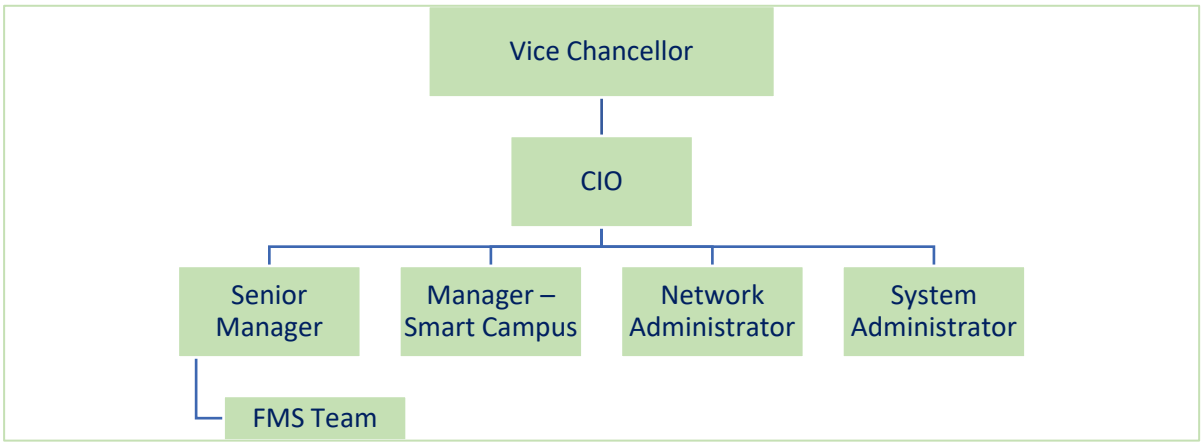
2. **Organization Structure**

Purpose:

a) To explain the organization structure of IT @DSU,
b) To define the roles and responsibilities for various functions within IT @DSU

IT Organizational Chart

The IT organizational structure @DSU is as shown below:



Responsibility

The various roles and responsibilities for DSU IT personnel are defined as follows:

CIO

Primary Responsibility: Acts as the custodian of overall IT resources at DSU.

Functional Responsibilities:

A. Be the last word in any decision pertaining to the IT security of the University.
B. Uphold the dictum of IT ethics outlined in the policy.
C. Responsible for the IT Strategy alignment to DSU strategy.

Senior IT Manager

Primary Responsibilities:

A. Plan, implement and monitor IT infra for computing infrastructure and environment (computers, VM's, etc.) of the campus.
B. Plan and manage the IT infra for the new campus buildings.
C. Project management and ongoing IT operations of campus
D. Manage the FMS team.

Manager Smart Campus

Primary Responsibilities:

A. Plan, implement and monitor various initiatives for the smart campus, not limited to energy management.

System Admin (Servers, Application & Database Administrator)

Functional Responsibilities:

A. Perform periodic backups of user and operating system files.
B. Deletion or alteration of system- related files or processes that are jeopardizing the security of a user account or of the system as a whole.
C. Inspect, edit or delete private information (whether in the form of user accounts, files, processes, etc) as required, and dealing with incidents of suspected inappropriate use.
D. Apply patches and upgrades to operating systems and utilities as available.
E. Maintain production/uptime/hardware fault logs.
F. Trouble shooting of any hardware-related problems on Servers & PC's.
G. Fault isolation, installation and diagnosis of Server/PC hardware.
H. Co-ordinate with vendors for corrective maintenance of all hardware peripherals as and when required.
I. Ensure the maximum uptime of links, Internet and maintain the logs of uptime/downtime of this hardware,

Network Administrator (LAN/WAN)

Functional Responsibilities:

A. Install, maintain, administer, support and upgrade the networks (LAN/WAN),Firewall.
B. Configure LAN and WAN switches, Access Points, hubs, and routers.
C. Ensure uptime of networks and support the links for all the building blocks of campus.
D. Support helpdesk personnel for server and network related issues.
E. Evaluate network-monitoring tools and recommend relevant tools that will enhance the network and provide defined security.

IT FMS support /Helpdesk

Functional Responsibilities

A. Perform End user IT asset management.
B. Receive, assign and record support calls from users. Ensure that the problems are resolved within the stipulated time period.
C. Execute helpdesk activities and collect feedback through various mechanisms especially for day-to-day desktop support calls.
D. Implement and support the solutions based on the problem reported and follow change management processes as defined in change management.
E. Plan and caution the users well in advance about problems anticipated and changes that are planned before they are affected.

3. **IT Infrastructure Usage Policy**

This policy presents the responsible use of the Information Technology Infrastructure at DSU. Users of IT-infrastructure will be subject to the following acceptable use policy.

A. Student, Staff and Faculty with authorized accounts may use the computing and IT facilities for academic purposes, official University work, and for personal purposes so long as such use does not violate any law, University policy or IT act of the Government of India, does not interfere with the performance of University duties or work of an academic nature, does not result in commercial gain or private profit other than that allowed by the University.

B. Users are expected to respect the privacy of other users and they shall not allow any other person to use their password or share their account. It is the users' responsibility to protect their account from unauthorized use by changing passwords periodically. Sharing of passwords for any purpose whatsoever is strictly prohibited.

C. The assigned DSU e-mail address constitutes the users' official email id. To the extent possible, users are expected to use only their official email addresses for official communications with other members of the University and external officials/stakeholders.

D. Spamming or spreading malware is disallowed. All communication carried out using personal email ids is entirely the individual's responsibility.

E. Any violations of policy will be treated as academic misconduct, misdemeanour, or indiscipline as appropriate. Depending upon the nature of the violation, the University authorities may take an action by issuing a warning through disabling the account. In extreme cases, the account may be completely deleted and/ or the user prohibited access to IT facilities at DSU and/ or sent to the University disciplinary action committee as constituted by the University management.

F. The policy may change as and when it is considered required and new policies or the changes in policy will take effect immediately after a brief announcement by any means, e-mail, printed notices, or through the news groups.

G. All devices (laptops/desktops/tablets/mobiles) connecting to the University network will need to be registered with IT services.

H. Antivirus Software to be mandatory on all laptops/desktops connected to the University Network. Blocking of illegal/blacklisted/inappropriate sites will be updated on a continual basis.

I. Overall internet usage patterns will be tracked on a per user level, to the extent required by law. In addition, total bandwidth usage per user will be tracked and heavy users will be notified.

4. **BYOD (Bring your Own Device) Policy**

All devices connecting to the IT network will need to be registered with IT Services. This includes desktops, laptops, tablets, mobile phones and any other devices requiring network access, wired or wireless. This will ensure better management of the health of the network, as also enable compliance with provisions of the IT Act. For this registration, students will need to send their MAC ID from their official USN email ID. Similarly, the staff will provide the MAC ID's of their personal devices that needs to connect to the University Internet.

5. **Printer Policy**

Users (Faculty & Staff) will make use of common network printers. Dedicated printer will be provided only for certain confidential and administrative printing post approval from Registrar office**.** Count of prints per user will be monitored and can be controlled as per directive of management. Default printing colour should be black. Colour printing permissions can be controlled and managed in compliance with organizational policies.

6. **License Management Policy**

This policy applies to procured software, evaluation software, software on loan from Industry partners and freeware. This policy explicitly states that DSU shall use only licensed and approved software and follow policies and procedures outlined below.

A. Software in DSU will be duly licensed for use as per legal compliances and regulatory directives. The IT department through the Registrar's office will be acquiring and managing licenses in DSU.

B. Evaluation software and Software on loan from Industry partners shall be used as per the terms and conditions specified.

C. Freeware shall be permitted for use provided it is authorized by the IT department. Students & Staff will be held responsible for any unlicensed software found on their devices. Users using unauthorized software may be liable for disciplinary action.

D. Evaluation software is acquired to assess the functionality and relevance of such software to either a task/project specific or the University as a whole, such software may be acquired on physical media, or downloaded from the internet.

E. The responsibility of license management rests with the system/network administrators.

F. Maintaining the sanctity of license is the responsibility of end users including faculty, staff and students. Any Student/Staff found to have violated this policy may be subject to disciplinary action.

7. **Password Policy**

The purpose of this policy is to establish a standard for creation of strong passwords, protection of those passwords, and the frequency of change. The scope of this policy includes all personnel who have or are responsible using the DSU network, or stores any non-public information. This includes users on Windows or UNIX platform/Linux plat forms (Multiplatform environment).

A. The Policy states that, the information assets of DSU would not be compromised because of weak passwords in systems and infrastructure devices which host it.

B. As a policy - all logon IDs in DSU domain should have a strong password. User is responsible for all actions and functions performed by his/her account.

C. All students and Staff are responsible for strictly adhering to the policy guidelines mentioned.

D. Any Student/Staff found to have violated this policy may be subject to disciplinary action.

8. **Internet & Intranet Security Policy**

The purpose of this policy is to establish management direction to procedures and requirements to ensure appropriate protection of DSU information and equipment by Internet & Intranet connections. This policy applies to all faculty, staff, students, employees, incubation companies' staff, contractors, consultants, temporaries, and other users at DSU Network, including third parties who access DSU computer networks.

DSU's Network encourages its users (Students & Staff) to explore the Internet wisely. Based on the usage pattern and status of Bandwidth, DSU can implement web filtering of certain sites. Such list will be published to the Staff & Students and will be updated on regular basis.

A. It is the responsibility of IT dept to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.

B. IT department reserves the right to exclude from Internet, the access to those services that have no reasonable relationship to the functioning of DSU.

C. Using DSU Internet facilities or equipment to make abusive, unethical or "inappropriate" use of the Internet shall not be acceptable. Examples of inappropriate employee Internet use include, but are not limited to, the following:

a) Conducting or participating in illegal activities like gambling.
b) Solicitations for any purpose which are not expressly approved by University management.
c) Revealing or publicizing proprietary or confidential information.
d) Representing personal opinions as those of the University.
e) Making or posting indecent remarks
f) Uploading or downloading commercial software in violation of its copyright.

D. To prevent any appearance of inappropriate conduct on the Internet and to reduce risk exposures to the organization, users shall not:

a) Enter into contractual agreements via the Internet ; e.g. enter into binding contracts on behalf of the University over the Internet without approval of DSU Management.
b) Use the University logos or the University materials in any web page or Internet posting unless it has been approved, in advance, by the DSU Management.
c) Attempt to gain illegal access to remote systems on the Internet.
d) Attempt to inappropriately telnet to or port scan remote systems on the Internet.
e) Establish Internet or other external network connections that could allow other organisation users to gain access into DSU systems and information assets.

E. Users (Students & Staff) must:

a) Not permit any unauthorized individual to obtain access to DSU Network Internet Connections.
b) Not use DSU Network Internet resources (software/hardware or data) for other than authorized University purposes.
c) Ensure that data under his/her control and/or direction is properly safeguarded according to its level of sensitivity.
d) Make backups of all sensitive, critical, and valuable data files as often as is deemed necessary. Use the Gdrive

F. All software downloaded from non DSU Network sources via the Internet must be screened with virus detection software prior to being opened or whenever the provider of the software is not trusted, downloaded software should be tested on a stand-alone (not connected to the network) non-production machine.

G. At any time and without prior notice, management/IT staff reserves the right to examine email, personal file directories, and other information stored on computers. This examination assures compliance with internal policies, supports investigations.

H. Violations of these policies can lead to revocation of system privileges and/or disciplinary action.

9. **Antivirus Policy**

This policy is to ensure that DSU's confidential information and technologies are not compromised, and that production services and other DSU interests are protected from Viruses, Malware, Worms & Trojans. This policy is applicable to all the users of the DSU network.

A. All devices like desktops and laptops are connected to the University network will need to have antivirus protection.
B. The Antivirus licensed by the University will need to installed on all connected machines. This will be tracked and enforced by the IT group, and machines violating this will be taken off the network until they are made compliant.
C. The virus scanner shall be scheduled to run to scan for viruses at regular intervals.
D. Antivirus activities shall be centrally managed. Central monitoring and logging console shall be deployed, to monitor the status of pattern updates on all the computers and to log the activities performed on them.
E. Anti-virus software scanning engine and the virus signature files shall be kept up to date.
F. Periodic audit on all the users' desktops and laptops shall be performed.
G. Containment and Managing of virus incidents

    a) In the event of a virus outbreak, System-admin or IT Staff shall initiate appropriate action to contain virus infections and assist in their removal.
    b) Virus-infected computers shall be removed from the network as soon as they are identified, until they are verified as virus-free.

10. **Physical Security**

This policy details the physical and environmental criteria necessary to protect sensitive IT systems and assets of DSU. This policy applies to all stakeholders of DSU.

A. Only authorized individuals shall have access to DSU's physical information systems resources.
B. Controls for restricted software programs shall be established and enforced to prevent authorized use reproduction, and modification.
C. Access to the DSU'S systems through remote connectivity is restricted and requires authorization by the IT Team or appropriate management.
D. Users are responsible for their IT devices inside and outside the University campus.
E. The movement of personnel can be regulated by way of installing access card mechanisms or biometric based systems.

If anyone is found violating this policy, strict disciplinary action would be taken.

11. **Network Security**

The scope of the policy encompasses the students, staff and all the systems/network administrators of DSU.

A. Reasonable precautions will be implemented so that DSU Information, while in transit, cannot be observed, tampered with, or extracted from the DSU computing and communication network by some unauthorized person or device.

B. All network-attached devices and communication lines must be authorized in order to access the DSU computing and communication networks. Change control procedures will be documented, and utilized for all DSU computing and communications networks.

C. Audit logs will be created, maintained, protected, and reviewed at periodic intervals.

D. Students & Staff who are authorized to use DSU computing and communication networks or general information resources, must act responsibly when using network resources consistent with DSU ethics policies and requirements for the conduct of students & staff.

E. Users are expected to access only those DSU computing and communication resources for which they are authorized. Information in any form is considered an asset of the University and must be protected. This protection of Information includes controlling the transmission of information over communication networks and guarding the computing and communication networks and servers from unauthorized access and intrusion from unauthorized users.

F. The access and security provisions for specific communication networks will be documented and incorporated into specific procedures and control mechanisms, general requirements are as follows:

a) Encrypt any DSU classified information transmitted externally via communication networks.

b) Use security mechanisms (eg. virus protection) in order to prevent the corruption of DSU Information.

c) Grant access to external communication networks through approved IT procedures.

d) Access only those systems and networks for which you have been authorized.

e) Protect all Information according to the provisions of the Information Security Practices relating to the authorized release of Information including any electronic Distribution.

f) Computing and communication resources are solely for Academic use. Limited personal use is permitted so long as it is reasonable, ethical, does not interfere with work / academic responsibilities or violate any laws under

a. The Information Technology (IT) Act, 2000,
b. The Information Technology (Intermediaries Guidelines) Rules, 2011,
c. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

The user will be personally responsible for any violation of the above laws.