IT Security Policy Ver-1.0

Release Control

Release Date	Version No:	Details	Released by:	Approved by:
September 21, 2021	V 0.1	Pre-release, the purpose of pre-release is to inform all stake holders about the issuance of this policy and also to give advance intimation to the assured departments to get prepared.	Mr. Joyjit Roy Ghatak Choudhury, Consultant (IT) - DSEU Mr. Prasun Kumar Assistant Registrar (IT) - DSEU	
November 17, 2021	V 1.0	First release	Mr. Ashwani Kansal, Registrar-DSEU	Dr. Neharika Vohra, Vice Chancellor-DSEU

Policy Owner

Department:	Represented by:	Date
Registrar-DSEU	Mr. Ashwani Kansal	November 17, 2021

Policy assured by :

Department:	Represented by:	Applicable to	Date
Directors / HODs	Individual Role Holders	Respective users using computing assets.	November 17, 2021

Table of Contents

1. OBJECTIVE

The purpose of this IT Security Policy is to protect the information assets of Delhi Skill and Entrepreneurship University (DSEU) from all threats, internal or external, deliberate or accidental. The policy is aimed at the Institution,

- Help safeguarding the availability, confidentiality and integrity of the University's information systems.
- Protecting the IT assets and services of the University against unauthorized access, intrusion, disruption or other damage.
- Ensuring compliance with applicable legislation and regulations.
- Providing a governance with clear responsibility and accountability.
- Designating the appropriate level of security requirements for securing Data and IT Resources.
- Help safeguarding University information technology resources ("IT Resources") from accidental or intentional damage and Data from alteration or theft

2. SCOPE

This policy applies to everyone (including, but not limited to, all DSEU faculty, staff, students, visitors, vendors, contractors, and employees of an affiliated entity) who accesses Data or University networks or who stores Data through the use of DSEU credentials or under the authority of and pursuant to University contracts.

This policy also applies to such access and storage by DSEU Community Members whether the Data is accessed, stored or otherwise resides on University owned or controlled devices, personally owned or controlled devices, or devices owned or controlled by a third party under contract with the DSEU.

3. USER RIGHTS AND RESPONSIBILITIES

DSEU has a responsibility for safe guarding the confidentiality of information through the protection of information from unauthorized disclosure with access only by entitlement.

All users, students and staff are required to demonstrate compliance to Security Policy, in order to protect the confidentiality, integrity, and availability of DSEU's IT Assets.

This policy also extends to contractors, consultants and / or 3rd parties providing services to DSEU.

DSEU Centralized IT Services Team is responsible for administering the information security functions in DSEU network using various IT security tools and appliances.

4. DEFINITIONS

Authorization – the function of establishing an individual's privilege levels to access and/or handle information.
Availability – ensuring that information is ready and suitable for use.
Confidentiality – ensuring that information is kept in strict privacy.
Integrity – ensuring the accuracy, completeness, and consistency of information.
Unauthorized access – looking up, reviewing, copying, modifying, deleting, analyzing, or handling information without proper authorization and legitimate business need.
University Information – information that DSEU collects, possesses, or has access to, regardless of its source. This includes information contained in hard copy documents or other media, communicated over voice or data networks, or exchanged in conversation.

5. POLICY DETAILS

5.1. USER AUTHENTICANTION & ACCESS

The DSEU expects members of its faculty, staff, and student body to understand and mitigate the IT security risks inherent in digital technologies. DSEU also requires members of its faculty, staff, and student body to protect DSEU's resources that include information assets, software, hardware, and facilities by adhering to the Information Security guidelines.

5.1.1 All members of DSEU including consultants, outside vendors and visitors to campus who have access to DSEU owned or managed information through computing systems or devices must maintain the security of that information and those systems and devices.

5.1.2 Respective HOD/Head should ensure that the sensitive Information, in all forms – written, electronically recorded, or printed – are protected from accidental or intentional unauthorized modification, destruction, or disclosure. Appropriate access and security controls to be followed in transmission and storage of any confidential data and adequate precautions to be taken to ensure that only the intended recipient can access the data.

5.1.3 Backups are a must for any organization, especially considering regulatory compliance and the ever-increasing cyber security threats for which businesses are at high risk. Respective individuals should ensure that reliable backup and data recovery strategy is in place for ensuring the confidentiality, integrity, and availability of their critical data related to academic / research / business process.

5.1.4 Departments / Business units will never ask for full details of any member's password or other security credentials and therefore, the users should never share their passwords to others.

5.1.5 Individuals to ensure that their respective computing assets that are connected to DSEU network have been protected with appropriate licensed anti-virus and anti-malware tools & all patched updated.

- Authentication is required for each connection to the network. Single sign-on through Web Login allows for a safe and secure computing environment with an added layer of protection.
- Access management using groups and role-based provisioning; for application and service providers.
- Do not leave your computer unattended without locking your computer or logging off.
- User must follow best practices to prevent misuse, loss or unauthorized access to systems:
  - Keep passwords confidential
  - Change passwords regularly
  - Never write down passwords
  - Never send passwords via email, fax or post
  - Change temporary passwords at first logon

5.2 NETWORK SECURITY AND MONITORING

- All IT assets in DSEU which includes but is not limited to: servers, workstations, and network access devices are subject to ongoing monitoring by IT Department. The inappropriate use of these systems and/or networks which violates the University's policies or local, state and federal laws will be investigated as needed. The Registrar may authorize the IT Team to conduct such IT security investigations.
- Automated tools will be used to monitor the DSEU network on real time for any notification of detected security events and vulnerabilities for following
  - Internet traffic
  - Electronic mail traffic
  - LAN traffic, protocols, and IT inventory
  - System security parameters
- Where feasible, the following files will be checked for signs of security issues and vulnerability exploitation at a frequency determined by risk:
  - Intrusion detection system logs
  - Firewall logs
  - User account logs
  - Network scanning logs
  - System error logs
  - Application logs
  - Data backup and recovery logs
  - Help Desk trouble tickets
  - Internet access logs
- Campus Directors/HODs to ensure that their respective department's computing assets that are connected to DSEU network to have:
  - Anti-virus installed and up-to-date for personal devices
  - Operating System patched with latest security updates

5.3 BACKUP AND DATA RECOVERY

- All DSEU systems, applications and data must be backed up on a technically practicable schedule suitable to the criticality, integrity, and availability requirements, as required by the respective data owners/faculty/Offices. Individuals should be responsible for taking their own backups.
- Information owners of business units, faculty/offices must ensure that appropriate backup and system recovery measures are in place for their business and academic data.
- In case, the backups are stored off site, appropriate security measures must be taken to protect against unauthorized disclosure or loss. Recovery procedures should be tested on a regular basis by the data owners.
- Backups of confidential or sensitive information to be encrypted
- Retention period of backups should be proportionate to the criticality, integrity, and availability needs of the data OR as decided by data owners.
- Backup and recovery documentation must be maintained and periodically reviewed by respective office HODs.

5.4 DATA PROTECTION

- All sensitive information that is transmitted or received by DSEU computer systems, including mobile devices, must be encrypted when transmitted over wireless or Public Networks, including when transmitted via FTP and electronic mail.
- Sensitive information should be saved in folders with access limited to those individuals authorized to access the information.
- Users must logoff or lock their workstations when not in use.
- Respective HODs / faculty is responsible for the processing and storage of the information or data in their respective computing devices for their academic and business purpose. The data protection should meet regulations guidelines of both domestic and international bodies.
- The data protection is to abide the provisions contained in different applicable Indian statutes, eg. IT Act, 2000 (as amended by the IT Act, 2008) and IT [Reasonable Security Practices And Procedures And Sensitive Personal Data or Information] Rules, 2011, & any other, to keep the data intact.

5.5 ADHERENCE WITH CENTRAL, STATE, LOCAL, CYBER AND APPLICABLE INTERNATIONAL LAWS

As a member of the DSEU community, you are expected to uphold local acts/ordinances and central, state, cyber and applicable international laws. DSEU guidelines related to use of technologies derive from this concern, including laws regarding license, copyright and the protection of intellectual property. As a user of DSEU's computing and network resources you must:

5.5.1. Abide by all Central, State, Local, Cyber and applicable International Laws.

5.5.2. Abide by all applicable copyright laws and licenses. DSEU has entered into legal agreements or contracts for many of our software and network resources which require each individual using them to comply with those end user agreements.

5.5.3. Observe the copyright law as it applies to music, videos, games, images, texts and other media in both personal use and in production of electronic information as the ease with which electronic materials can be copied, modified and sent over the Internet makes electronic materials extremely vulnerable to unauthorized access, invasion of privacy and copyright infringement.

5.5.4. You should not use, copy, or distribute copyrighted works (including but not limited to Web page graphics, sound files, film clips, trademarks, software and logos) unless you have a legal right to use, copy, distribute, or otherwise exploit the copyrighted work. Doing so may provide the basis for disciplinary action, civil litigation and criminal prosecution.

5.5.5. You should not use DSEU computing and network resources for illegal activities.

5.6 ENFORCEMENT AND COMPLIANCE

Non-compliance with security policy and guidelines can bring about significant risk and liability for DSEU, which puts the institution at significant risk of legal action, substantial penalty and substantial damage to brand name as a whole.

Violation of this Policy may result in suspension or loss of the violator’s use privileges, with respect to Institutional Data and University owned Information Systems. Additional administrative sanctions may apply up to and including termination of employment or contractor status with DSEU. Civil, criminal and equitable remedies may apply.

Registrar-DSEU reserves the right to direct IT Office to inspect a faculty or staff member’s computer system for violations of this policy. Periodic, random audits shall also be conducted as appropriate and as advised to IT Office.

If an individual is found to be in violation of this policy, the concerned authority of DSEU will take disciplinary action, including the restriction and possible loss of network privileges. A serious violation could result in more serious consequences, up to and including suspension or termination from the University.

You can report any violations of the IT Security Policy at abuseinfo@dseu.ac.in

DSEU Conditions to follow the IT security policy. Failure to comply with these could constitute a disciplinary offence. The Registrar-DSEU reserves the right to authorize IT support team to audit without notice to enable them to check against

- Any unlicensed software or hardware or illicit copies of documentation
- Suspect a computer used for official work or study has committed a security breach or is under attack

- Reporting an email spam or phishing attempt
- Reporting unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information and is reasonably believed to result in loss or injury.
- Reporting a breach of personal data when it leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any information relating to an identified or identifiable natural person (“personal data”) transmitted, stored or otherwise processed by or on behalf of the organization.