Password Policy Ver-1.0

Release Control

Release Date	Version No:	Details	Released by:	Approved by:
October 19, 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
Information Technology	Assistant Registrar – IT, DSEU	All users	November 17, 2021

Table of Contents

1. OBJECTIVE

The purpose of this document is to provide a set of minimum security standards governing the use of passwords for Delhi Skill & Entrepreneurship University (DSEU) information technology systems to ensure that passwords used to access computer resources are selected and updated in line with best proactive security standards.

This document is intended to offer minimum standards for system and application administrators and developers. All parties are encouraged to apply more stringent controls than those outlined below in accordance with the security needs of the system and the information being stored or accessed. Regulatory, compliance, or grant requirements supersede any standards defined below.

Users must take all necessary steps to protect and maintain the security of any equipment, software, data, storage area and/or passwords allocated for their use. This policy dictates the minimum that a user must do to conform to this requirement when selecting and updating a password.

Password policies are used to mitigate possible attacks against the University IT infrastructure and the data held upon it. Use of long, complex passwords helps to mitigate attacks that attempt to guess passwords, and regular password changes to mitigate long term exploitation of any disclosed or discovered passwords.

Passwords are a critical aspect of computer security forming the front line of protection for user accounts. A poorly chosen password can result in the compromise of DSEU's entire network.

As such, all DSEU students and employees (including contractors and vendors with access to DSEU systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. SCOPE

The scope of this policy includes all users who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any DSEU facility, has access to the DSEU network, or stores any non-public DSEU information. External parties that provide information processing services to the University

The policy will be communicated to users and relevant external parties.

3. USER RIGHTS AND RESPONSIBILITIES

Individuals are responsible for keeping passwords secure and confidential. As such, the following principles must be adhered to for creating and safeguarding passwords:

- E-mail passwords must be changed immediately upon issuance for the first-use. Initial passwords must be securely transmitted to the individual.

- Passwords must never be shared with another individual for any reason or in any manner not consistent with this policy. A shared or compromised password must be reported to IT security incident

- Users including Employees / Visiting Faculty / Contracts / Interns / Students, must never ask anyone else for their password. If you are asked to provide your password to an individual or sign into a system and provide access to someone else under your login, you are obligated to report this to the Privacy Office or IT Security by e-mail to abuseinfo@dseu.ac.in

- Passwords must never be written down and left in a location easily accessible or visible to others. This includes both paper and digital formats on untagged (unsupported) devices.

- Individuals must never leave themselves logged into an application or system where someone else can unknowingly use their account.

- Passwords must be unique and different from passwords used for other personal services (e.g., banking).

- Passwords must meet the requirements outlined in this policy.

- Passwords must be changed at the regularly scheduled time interval of 180 days or upon suspicion or confirmation of a compromise.

- In the event that a password needs to be issued to a remote user or service provider, the password must be sent with proper safeguards (e.g., shared via a secure password manager or sent via an encrypted email message).

- If a password needs to be shared for servicing, IT Support should be contacted for authorization and appropriate instruction.

- Individuals with access to service accounts or test accounts must ensure the account password complies with this policy.

In the event a breach or compromise is suspected, the incident must be reported to IT Support immediately.

IT Team will never ask for a password. In IT support scenarios where an IT account cannot be used, an individual may allow a technician to utilize his/her computer under the individual's account even if the individual is unable to be present during the entire support session. The individual should not share his/her password with the technician.

All IT support technicians are expected to abide by the Acceptable Use of Information Technology Resources policy and their actions may be audited upon request.

In the event of a hardware malfunction and the device needs to be repaired by a third-party, the device hard drive should be backed up to a secure storage device and wiped securely prior to being handed over to an external technician. IT Support can assist with a secure backup and the drive erasure and other exceptional circumstances. Passwords should not be shared with an external technician.

Computing accounts shall be protected by strong passwords. Account holders and system administrators shall protect the security of those passwords by managing passwords in a responsible fashion. System developers shall develop systems that store or transmit password data responsibly and that use secure authentication and authorization methods to control access to accounts.

4. POLICY DETAILS

4.1. GENERAL INFORMATION

Under no circumstances should a user divulge their password to another person.

1. All system-level passwords (e.g., root, enable, admin, application administration accounts, etc.) must be changed on at least a semi-annual basis.
2. All production system-level passwords must be part of the IT Services administered global password management database.
3. All user-level passwords (e.g., email, web, desktop computer, etc.) must
    1. Maximum password age of 180 days
    2. Exhibit complexity by
        1. Not contain all or part of the user's account name
        2. Contain characters from all of the following four categories:
            1. Uppercase characters (A through Z)
            2. Lowercase characters (a through z)
            3. Base 10 digits (0 through 9)
            4. Non-alphabetic characters (for example, !, $, #, %)
        3. Maintain a password history of 5 passwords and not allow reuse
        4. Must be a minimum of 8 characters
        5. Be locked out if more than 3 unsuccessful attempted logons
        6. Username and password combinations must not be inserted into email messages or other forms of electronic communication unless the message is encrypted.
        7. All temporary passwords must be changed at first login.
        8. If an account or password is suspected to have been compromised, report the incident to IT Services and immediately change all of the associated passwords.
        9. Accounts created for use on external online resources must not use the same password for University authentication.
        10. Passwords must not be something that can easily by guessed (avoid using your name, children or a pet’s name, car registration number, football team, date of birth, calling name etc).

4.2 CHANGING PASSWORD

Passwords must be changed regularly to mitigate the long term exploitation of any disclosed or discovered passwords. It is recommended those passwords are changed every 180 days.

4.3 PASSWORD USE

Passwords are the mechanism used to protect the security of University systems and must be protected.

- Passwords must be kept secret.
- Passwords must not be written in a form that others could identify.
- Passwords must not be stored electronically in a non-encrypted format.
- Passwords must never be shared with others.
- Care should be taken to prevent anyone from watching you type your password.

4.4 ACCOUNT LOCKOUT

In order to limit attempts at guessing passwords or compromising accounts, an account lockout policy will be in effect for all systems. Account lockout thresholds and durations vary based on the type of user, as defined below.

- Accounts will lockout after six (3) invalid password attempts in fifteen (15) minutes.
- Accounts will remain locked for a duration of thirty (30) minutes, unless the IT Support is contacted and the user's identity is verified in order for the account to be unlocked sooner.

4.5. ADHERENCE WITH CENTRAL, STATE, LOCAL, CYBER AND APPLICABLE INTERNATIONAL LAWS

As a member of the DSEU community, you are expected to uphold local ordinances and central, state, cyber and applicable international laws. DSEU's guidelines related to use of technologies derived 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:

- Abide by all Indian Central, State, Local, Cyber Law and applicable International Laws.
- Abide by all applicable copyright laws and licenses & protect the related passwords.
- 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 agreements.

4.6. ENFORCEMENT AND COMPLIANCE

Violations of this policy may incur some type of disciplinary measures as violations of other University policies, and severity of the punishment will be decided by the competent authority.

Systems and accounts that are found to be in violation of this policy may be removed from the DSEU network and the account will be disabled until the systems or accounts can comply with this policy.

Each University department / unit is responsible for implementing, reviewing and monitoring internal policies, practices, etc. to assure compliance with this Policy.

The Registrar of the University will be responsible for the enforcement of the Policy.