

PASSWORD POLICY

Document Title:	Password Policy
Document ID:	IST/DIR/ISP/004
Document Type:	LUMS Policy
Owner:	Head – IT Operations
Approval Authority:	Director – Information, Systems & Technology
Approval Date:	
Effective Date:	
Version Number:	02
Last Review Date:	May 21, 2026
Next Review Date:	

CHANGE RECORD

Author	Version	Change Reference	Date
Muhammad Mohsin Abbas	00	Draft policy prepared	05/03/2018
Khubaib Nazir	00	Draft Review & Approval	05/03/2018
Iffat Chaudhry	00	Review of the draft policy	27/05/2024
Faisal Kheiri	00	Review and edits	30/05/2024
Talal Javed	00	Initial Review and feedback	30/05/2024
Faisal Kheiri	1.2	Removal of Password Expiry	05/09/2024
Faisal Kheiri	2.0	Approval of Policy- v 2.0	21/05/2026

APPROVALS

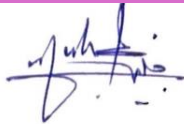
Name	Designation	Signature	Date
Khubaib Nazir	Head of IT Operations		
Faisal Kheiri	Director - IST		21-05-2026

Table of Contents

1. Purpose	3
2. Scope	3
3. Policy Statement(s)	3
4. Guidelines	4
5. Waiver of Policy	4
6. Exemptions and Revisions	4
7. Roles and Responsibilities of Policy Implementation	5
8. Title of Position with Maintenance Responsibility	5
9. Non-Compliance with Policy	5
10. Related Documents/Policies	5
11. Distribution and Physical Security	5
12. Contacts	5

LUMS PASSWORD POLICY

1. Purpose

The policy governs the composition, allocation, and renewal of passwords issued to LUMS faculty, staff, students, and guests to access IT services, including the network and core applications.

2. Scope

This policy is applicable across the University and applies to all students, faculty, staff, alumni, and participants who attend workshops, seminars, courses, and events including special groups, centers, and organizations accessing LUMS network and IT services.

It applies to all LUMS enterprise systems (computers, email, LUMS website, Zambeel, SAP, Admissions and FA System, CES, REDC, GAMES, etc.).

3. Policy Statement(s)

The following controls must be implemented regarding secret authentication/passwords:

1. The minimum length of the password must be eight (8) characters.
2. Passwords will be checked for the inclusion of at least 3 of the following 4 categories
 - Upper-case alphabets (A-Z)
 - Lower-case alphabets (a-z)
 - Base 10 digits (0-9)
 - Special characters (e.g.!, @, #, \$, ^, &, etc.)
3. Passwords will never expire unless there is a need to reset them due to security concerns. However, for SAP, the password will expire after 90 days. Two Factor Authentication (2FA) will apply to the LUMS e-portal, which contains sensitive information (salaries, personal details, budget, loan details, etc.). Email password MFA is enabled, but optional to avail by respective users.
4. Password history is maintained, and users are not allowed to repeat any of their 3 most recently used passwords.
5. A password cannot contain in entirety or a portion of the username.
6. The account will be locked for 5 minutes after three unsuccessful attempts.
7. Authentication systems (Active Directory, SAP, etc.) will be configured to enforce system-related policies across the university.
8. For accounts that access confidential and sensitive information, it is highly recommended to enable multi-factor authentication.

4. Guidelines

Users of LUMS business applications and other information systems/services shall be required to follow good security practices in selecting and using passwords. The following guidelines shall govern password usage.

Users shall be required to:

1. Keep the password confidential
2. Change passwords whenever there is any indication of possible system or password compromise
3. Select strong passwords with a minimum length of 8 characters
4. Avoid re-using or cycling old passwords
5. Change temporary passwords at the first log-on
6. Do not include passwords in any automated log-on process, e.g. stored in a macro or function key
7. Do not use the same password for business and non-business purposes.
8. Single sign-on should be used for all services only when it is ensured that a reasonable level of protection has been established for the storage of the password within each service, system, or platform
 - In addition to the rules stated above, the following are a few Do nots to keep in mind when choosing passwords: **Do not** choose a password that is a dictionary word (English or foreign)
 - **Do not** choose a password that is the name of a family member, pet, or friend, DoB, telephone, etc.
 - **Do not** choose keyboard, word, or number sequences as passwords (e.g. 12345678, qwerty, asdfg, aaaaa, etc.)
 - **Do not** choose passwords that are hybrids of the above
 - **Do not** choose passwords that are any of the above spelled backward
 - **Do not** choose passwords that are any of the above followed or preceded by a digit (e.g. 1password, password1, etc.)
 - **Do not** share passwords with anyone
 - **Do not** insert passwords in e-mails
 - **Do not** write down passwords in easily accessible places

5. Waiver of Policy

The LUMS Vice Chancellor may waive a part or whole of the policy subject to any conditions or restrictions as they may deem fit and appropriate.

6. Exemptions and Revisions

The University, its officers, or any other person or entity associated with them shall have no liability whatsoever for any losses, damages, claims, legal costs, or other expenses that a person may suffer or incur, whether directly or indirectly (including any loss of profit or damage to reputation) by reason of any proceedings instituted or measures taken pursuant to these procedures.

The provisions of this Policy may be revised or amended by the University from time to time in its sole and absolute discretion provided that any such revision or amendment in the Policy shall not apply to any proceedings that have commenced or affect the validity of any decision made, action taken, direction given, proceedings taken, instrument executed, penalty or punishment imposed or anything done lawfully and conclusively prior to the said revision or amendment.

7. Roles and Responsibilities of Policy Implementation

Roles and responsibilities with respect to the personnel involved in policy are described in the attached Annexure.

8. Title of Position with Maintenance Responsibility

IST's Governance, Risk, and Compliance section shall be responsible for the maintenance of the Policy including its periodic review and approval of any subsequent modifications to the said policy.

9. Non-Compliance with Policy

Disciplinary process by the University shall be initiated in case non-compliance of policies and procedures is identified.

10. Related Documents/Policies

None

11. Distribution and Physical Security

Access to policies and procedures on the intranet portal shall be restricted and access shall be provided by the Policy Owner through the LUMS Access Management Process. For further information, refer to the Access Management Policies and Procedures. However, in case a hard copy is required, printing rights shall be granted to the respective stakeholder as part of the standard Access Management Process.

Where there is a change in responsibility of an employee, the copy/access that the employee has of the policy document should be handed over to the new employee and this action shall be documented in the previous employee's handing over notes. When an employee leaves the employment of LUMS, then the copy of/access to the policy document should be returned to/revoked by the Head of Department/IST Department prior to his departure.

12. Contacts

Contact	Designation	Email
Muhammad Khubaib Nazir	Head of IT Operations (IST)	khubaib@lums.edu.pk
Iffat Chaudhry	Manager, Governance, Risk & Compliance	iffat@lums.edu.pk