

ACCESS CONTROL POLICY

Document Title:	Access Control Policy
Document ID:	IST/DIR/ISP/002
Document Type:	Unit Level Policy
Owner:	Head – Cyber Security (IST)
Approval Authority:	Director – Information, Systems & Technology
Approval Date:	
Effective Date:	
Version Number:	00
Last Review Date:	
Next Review Date:	

CHANGE RECORD

Author	Version	Change Reference	Date
Tariq Sheikh	00	Draft policy prepared	11-12-2023
Iffat Chaudhry	00	Review of the draft policy	29-12-2023
Talal Javed	00	Review of the draft policy	23-05-2024
Faisal Kheiri	00	Review of the draft policy	30-05-2024

APPROVALS



Name	Designation	Signature	Date
Tariq Sheikh	Head–Cyber Security (IST)		June 4, 2024
Faisal Kheiri	Director - IST		June 4, 2024

Table of Contents

Access Control Policy	3
1. Purpose	3
2. Scope	3
3. Policy	3
3.1 User Access Control	3
3.2 Network Access Controls	5
3.3 Systems Controls	6
4 Waiver of Policy	6
5 Exemptions and Revisions	6
6 Roles and Responsibilities of Policy Implementation	7
7 Title of Position with Maintenance Responsibility	7
8 Non-Compliance with Policy	7
9 Related Documents/Policies	7
10 Distribution and Physical Security	7
11 Contacts	7

Access Control Policy

1. Purpose

The purpose of this policy is to ensure that only authorized personnel are provided access to information and information processing facilities (including operating systems, databases, networks, and applications).

2. Scope

This policy applies to all employees, associated professionals, suppliers, internal and external auditors. Additionally, this policy applies to information assets that store, process, and manage data.

3. Policy

Access control activities shall be focused on and driven by this policy as part of the overall cybersecurity policy.

3.1 User Access Control Guidelines

- 3.1.1 Employ layered access controls by restricting access at the network, system, and associated services/application levels to prevent unauthorized access.
- 3.1.2 Design and implement authentication and identity verification mechanisms to minimize the opportunity for unauthorized access.
- 3.1.3 Control and monitor the creation, change, and termination of user access rights and associated privileges.
- 3.1.4 Define and document a process to authorize access to LUMS information processing facilities, ensuring access is granted only after completing the authorization process.
- 3.1.5 Maintain a formal record for examination of all users registered to use a LUMS system or information processing facility.
- 3.1.6 Authorize and approve access to LUMS information processing facilities and official information with proper business justification, providing the minimum level of privilege/access required for job responsibilities.
- 3.1.7 Require Line Managers to approve access requests before creating user IDs.
- 3.1.8 Assign access privileges, including administrator rights in accordance with the user's role and responsibilities maintained by their manager.
- 3.1.9 Conduct Periodic reviews to identify and remove or disable redundant and unused user IDs.

- 3.1.10 Restrict and authorize Group IDs or generic service IDs through Cybersecurity; deviations must be recorded with an audit trail.
- 3.1.11 Do not hard code Group IDs and generic IDs; follow defined policies for granting, modifying, or revoking access rights.
- 3.1.12 Implement a format User Access Management procedure to assign or revoke access rights for users on all systems and services, including:
 - a) Obtaining requests from HR for new joining or transfers.
 - b) Obtaining requests from HR/Line manager for access rights modification.
 - c) Line Managers provide approvals for their respective users.
 - d) Providing access by segregation of duties.
 - e) Avoiding the use of Group IDs unless approved by Head Cybersecurity.
 - f) Periodically reviewing access rights with owners of information systems or services.
- 3.1.13 Revoke and reassign access rights on a "need-to-have" and least privileges basis when there is a change in the role of a user or a transfer to another function.
- 3.1.14 Revoke the rights of users to access information systems or information processing facilities for accounts identified as no longer having authorized access or being inactive for:
 - a) More than 30 days for suppliers.
 - b) More than 90 days for LUMS employees.
- 3.1.15 Evaluate inactive accounts to identify their business need before revoking access rights.
- 3.1.16 Identify and document privileged access rights granted to users on each system or process.
- 3.1.17 Allocate privileged access rights on a need-to-use basis and on an event-by-event basis.
- 3.1.18 Follow the User Access Management procedure for granting access rights; review privileged access rights every three months (preferably every month) to ensure alignment with business and technical requirements.
- 3.1.19 Assign privileged access rights to a user ID different from those used for regular business activities; do not perform regular business activities from a privileged ID.
- 3.1.20 Log changes to privileged accounts and maintain an audit trail.
- 3.1.21 Review and adjust access rights and privileges granted to employees and suppliers in the case of termination or change of employment.

- 3.1.22 Raise a request and obtain approvals from the Line Manager for active accounts after an employee has resigned, for business reasons.
- 3.1.23 Ensure that access rights of users to information assets are revoked within 24 hours of separation or end of their employment, contract, or agreement.
- 3.1.24 Support any access granted as an exception with a valid justification and approval by the respective business heads.

3.2 Network Access Controls

Implement considerations for the use of networks and network services:

- 3.2.1 Grant access to users based on username and password authentication; use two-factor authentication mechanisms where applicable.
- 3.2.2 Follow User Access Management procedures for access to networks and network services.
- 3.2.3 Implement management controls and procedures to restrict access to network services.
- 3.2.4 Use secure means for access to network services and employ VPN for remote access.
- 3.2.5 Monitor and manage the use of network services.
- 3.2.6 Implement Firewall (including IPS/IDS) and web application firewall (WAF) functionality to protect the LUMS network from external attacks.
- 3.2.7 Use Active Directory (AD) or Light Weight Directory Access Protocol (LDAP) for authentication access to the LUMS network.
- 3.2.8 Create segregation between LUMS internal networks and external/public networks where applicable.
- 3.2.9 Apply secure authentication mechanisms for users accessing LUMS information systems; consider dual-factor authentication where applicable.
- 3.2.10 Monitor user access to network services and enforce an audit trail.
- 3.2.11 Provide access only to authorized network services.
- 3.2.12 Allocate access rights to information systems and services from initial registration/modification to final de-registration of users, including privileged access rights.

3.3 Systems Controls

- 3.3.1 Restrict, control, and track access to the program source code of operational systems and object libraries to prevent corruption of application programs.
- 3.3.2 Avoid holding program source libraries in operational systems where possible.
- 3.3.3 Follow appropriate version management/control processes for program source codes.
 - a) Exercise the right to audit compliance with such processes in the case of third-party systems.
 - b) Provide support personnel with restricted access to program source libraries
 - c) Carry out all updates or issuance of program source code to developers through an authorized request.
 - d) Ensure all personnel managing access have proper training.
- 3.3.4 Make this policy widely available to all users, including internal staff, outsourced staff, suppliers, and reference it in all Service Level Agreements (SLAs), Operational Level Agreements (OLAs), Underpinning Contracts (UCs), and Agreements.
- 3.3.5 Authorize this policy by top executive management within IT and the Board and endorse compliance on a regular basis.
- 3.3.6 Review and, if necessary, revise this policy on a required basis.
- 3.3.7 Ensure all Business and IT staff follow this policy.

4. 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.

5. 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.

6. Roles and Responsibilities of Policy Implementation

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

7. 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.

8. Non-Compliance with Policy

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

9. Related Documents/Policies

Annexure – User Access Right Procedures; Data Handling Procedure v1.3

10. 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.

4 Contacts

Contact	Designation	Email
Mr. Tariq Sheikh	Head – Cyber Security (IST)	tariq@lums.edu.pk
Mr. Talal Javed	Head – Data Analytics, Governance & Security (IST)	talal.javed@lums.edu.pk