

INFORMATION SECURITY POLICY

Document Title:	Information Security Policy
Document ID:	IST/DIR/ISP/001
Document Type:	Unit Level Policy
Owner:	Head – Cyber Security (IST)
Approval Authority:	Director – Information, Systems & Technology
Approval Date:	14-03-2024
Effective Date:	14-03-2024
Version Number:	00
Last Review Date:	12-03-2024
Next Review Date:	March 2026

CHANGE RECORD

Author	Version	Change Reference	Date
Tariq Sheikh	00	Draft policy prepared	11-12-2023
Iffat Chaudhry	00	Review of the draft policy	18-12-2023
Faisal Kheiri	00	Review of the draft policy	12-03-2024

APPROVALS


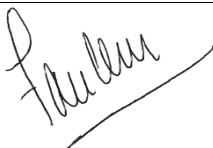
Name	Designation	Signature	Date
Tariq Sheikh	Head–Cyber Security (IST)		12-03-2024
Faisal Kheiri	Director - IST		14-03-2024

Table of Contents

Information Security Policy	3
1. Purpose	3
2. Scope	3
3. Policy	3
4. The List of Recommended Topic Specific Policies	4
5. Waiver of Policy	5
6. Exemptions and Revisions	5
7. Roles and Responsibilities of Policy Implementation	5
8. Title of Position with Maintenance Responsibility	5
9. Non-Compliance with Policy	6
10. Related Documents/Policies	6
11. Distribution and Physical Security	6
12. Contacts	6

Information Security Policy

1. Purpose

The objective of this policy is to articulate information security requirements for all information assets, whether physical, logical, or intangible, within LUMS. Serving as a guiding compass, this policy aims to provide clear directives for safeguarding information assets against potential threats, both internal and external, that pose risks to confidentiality, integrity, or availability.

2. Scope

This policy applies across the University and to individuals, processes, and technological systems that engage with information and its associated assets.

3. Policy

Information security activities shall be focused and overall driven by this policy:

1. LUMS management shall exhibit commitment through a information security governance structure, establishing an architecture ensuring alignment of LUMS's security programs with business objectives, compliance with regulations and standards, and achieving goals for managing security and risk.
2. LUMS management shall ensure the establishment of information security objectives in line with the Information security policy and aligned with business objectives.
3. LUMS management shall demonstrate commitment and provide the necessary resources to achieve information security objectives.
4. LUMS management shall ensure that management directives related to Information security are communicated through topic-specific policies* and implemented.
5. All internal staff, outsourced staff, suppliers, and third-party service providers shall share the commitment to providing appropriate levels of security across all functions holding LUMS and its customer information.
6. All internal staff, outsourced staff, suppliers, and third-party service providers shall share the obligation to protect information, assure customer privacy, and remain vigilant in preventing unauthorized or fraudulent activity.
7. A mechanism for collecting and analyzing information related to information security threats shall be established to produce threat intelligence and provide awareness of LUMS's threat environment, enabling appropriate mitigation actions.
8. Precautions and measures shall be always taken to ensure the Confidentiality, Integrity, and Availability of all information systems based on their importance for business activities.

9. Information assets shall be identified, and associated risks assessed and evaluated, with appropriate measures, implemented in risk treatment planning.
10. Rules for the secure development of software and systems shall be established and applied.
11. Backups shall be maintained for critical data according to classification to ensure business continuity without disruption.
12. Information and Communication Technologies (ICT) readiness shall be planned, implemented, maintained, and tested based on business continuity objectives and ICT continuity requirements.
13. A mechanism for reporting information security incidents shall be established for the timely resolution of Information security incidents.
14. Access to LUMS's information and associated assets shall be controlled through the unique identification of individuals and systems to enable the appropriate assignment of access rights; access rights shall be reviewed regularly to align with changing business needs.
15. Information security roles and responsibilities shall be clearly defined and documented.
16. An Information security training and awareness program shall be established and implemented.
17. LUMS shall comply with all applicable legal, statutory, regulatory, and contractual requirements related to Information security.
18. This policy shall be widely available to users, including internal staff, outsourced staff, and suppliers. Its compliance shall be referred to in all Service Level Agreements (SLAs), Operational Level Agreements (OLAs), Underpinning Contracts (UCs), and Agreements.
19. This policy shall be authorized by the top executive management within LUMS, and compliance shall be endorsed regularly.
20. This policy shall be reviewed and, where necessary, revised as required.
21. All Business and IT staff shall adhere to this policy.

4. The List of Recommended Topic Specific Policies

1. Access control policy
2. Malware defense policy
3. Information backup policy
4. Information transfer/exchange policy
5. Cryptographic controls policy
6. Information security incident and threat management policy
7. Physical security policy
8. Secure configuration and hardening policy
9. Network security policy
10. Technical vulnerability management policy
11. Information and document classification policy
12. Asset management policy

13. Secure development policy
14. Secure systems engineering policy.

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
Tariq Sheikh	Head – Cyber Security (IST)	tariq@lums.edu.pk
Faisal Kheiri	Director IST	faisal.kheiri@lums.edu.pk