LUMS
A Not-for-Profit University

# LUMS CYBER SECURITY FRAMEWORK & GOVERNANCE FRAMEWORK_V1.0

## Document Change Record

| Author | Version | Change Reference | Date |
|---|---|---|---|
| Tariq Sheikh | 00 | Draft Framework prepared | Sept 10, 2024 |
| Faisal Kheiri | 00 | Review of the draft Framework | Sept 23, 2024 |
| Iffat Chaudhry | 00 | Review of the draft Framework | Sept 24, 2024 |
| Talal Javed | 00 | Review of the draft Framework | Sept 24, 2024 |
| Faisal Kheiri | 00 | Approval of the Framework | Oct 11, 2024 |

LUMS
A Not-for-Profit University

# LUMS Cyber Security & Governance Framework

## 1. Introduction

### 1.1 Purpose

The purpose of this Cybersecurity Governance Framework is to establish a comprehensive approach to managing cybersecurity risks at LUMS. It aims to protect the university's information assets, ensure compliance with legal and regulatory requirements, and foster a culture of security awareness across the institution.

### 1.2 Scope

This framework applies to all faculty, staff, students, contractors, and third-party service providers who access, manage, or use university IT resources, including but not limited to computer systems, networks, and data.

### 1.3 Objectives

- Safeguard the confidentiality, integrity, and availability of university data
- Establish clear roles and responsibilities for cybersecurity governance.
- Ensure compliance with GDPR for our international memorandum of understanding (MoU)
- Promote security awareness and best practices among all users.

### 1.4 Governance Structure

#### 1.4.1 Roles and Responsibilities

- Head Cybersecurity: Responsible for overseeing the cybersecurity strategy and implementation across the university.
- IT Steering Committee: This committee consists of representatives from various departments who advise on cybersecurity policies, review security incidents, and recommend strategic actions. Meets every semester, however, gives email response on a need basis.
- Department Heads: Ensure compliance with cybersecurity policies within their respective departments.
- IST Staff: Implement security controls, monitor systems, and respond to incidents as defined in this framework.

- End Users (Faculty, Students, and Staff): Responsible for adhering to cybersecurity policies and reporting security incidents.

#### 1.4.2 Reporting Structure

The Head Cybersecurity reports directly to the Director Information Systems and Technology and provides updates to the university's leadership on cybersecurity matters. The IT Steering Committee closely works with the Head Cybersecurity, with regular briefings to senior management and if needed to the executive leadership (Management Committee).

## 2. Cybersecurity Policies (minimum set)

### 2.1 Acceptable Use Policy

Defines the acceptable use of university IT resources, including guidelines for internet access, email communication, and personal devices on the network.

### 2.2 Data Protection Policy

Outlines measures for protecting sensitive and personal data, including data classification, encryption, and access control standards.

### 2.3 Incident Response Policy

Establishes procedures for detecting, responding to, and recovering from cybersecurity incidents. Defines roles, responsibilities, and communication protocols during an incident.

### 2.4 Access Control Policy

Specifies how access to systems and data is managed, including user authentication, authorization processes, and the principle of least privilege.

### 2.5 Password Management Policy

List requirements for password complexity, frequency of changes, and best practices for password security.

LUMS
A Not-for-Profit University

## 3. Risk Management

### 3.1 Risk Assessment

Conduct regular risk assessments to identify potential threats and vulnerabilities to university systems. Assess the impact and likelihood of risks to prioritize mitigation efforts.

### 3.2 Risk Mitigation

Implement CIS-based security controls to reduce identified risks, including technical, administrative, and physical controls. Document the controls in a risk register.

### 3.3 Risk Acceptance

Define criteria for accepting risks that cannot be mitigated and establish a process for obtaining approval from executive leadership.

## 4. Compliance and Legal Requirements

### 4.1 Regulatory Compliance

Ensure compliance with applicable laws and regulations in consideration of GDPR data protection laws. Establish processes for regular compliance checks and audits.

### 4.2 Internal Audits

Conduct periodic internal audits to assess compliance with cybersecurity policies and identification of areas for improvement.

## 5. Incident Management

### 5.1 Incident Detection

Utilize monitoring tools and processes to detect potential security incidents. Ensure that systems are in place for logging and alerting people for suspicious activity.

### 5.2 Incident Response Plan

Define a step-by-step process for responding to incidents, including containment, eradication, recovery, and post-incident analysis. Ensure that contact lists and communication protocols are up to date.

### 5.3 Post-Incident Review

Conduct a review after each incident to identify lessons learned and update policies and controls to prevent future occurrences.

LUMS
A Not-for-Profit University

## 6. Security Awareness and Training

### 6.1 Training Programs

Develop and deliver regular cybersecurity training sessions for all faculty, staff, and students. Include topics such as phishing, password security, and data protection.

### 6.2 Phishing Simulations

Conduct periodic phishing simulations to assess user awareness and improve training efforts based on the results.

### 6.3 Policy Acknowledgement

Require all users to review and acknowledge their understanding of university cybersecurity policies as part of onboarding and annually thereafter.

## 7. Technology and Tools

### 7.1 Security Infrastructure

Deploy security technologies such as firewalls, intrusion detection, intrusion prevention systems, antivirus software, and endpoint protection solutions to safeguard university networks.

### 7.2 Monitoring and Logging

Implement continuous monitoring of network traffic, system logs, and user activities. Use Security Information and Event Management (SIEM) tools to aggregate and analyze logs for security incidents.

### 7.3 Vulnerability Management

Regularly conduct vulnerability scans and penetration tests to identify and remediate security weaknesses. Ensure prompt patching of software and systems.

## 8. Data Governance

### 8.1 Data Classification

Define and implement a data classification scheme to categorize data based on sensitivity levels (e.g., public, internal, confidential, and restricted).

### 8.2 Data Lifecycle Management

Establish guidelines for the storage, access, retention, and secure disposal of data throughout its lifecycle.

### 8.3 Encryption Standards

Mandate encryption for sensitive data, both at rest and in transit to protect against unauthorized access.

## 9. Third-Party Management

### 9.1 Vendor Risk Assessment

Evaluate third-party service providers for security risks before engaging their services. Require cybersecurity assessments as part of the procurement process.

### 9.2 Service Level Agreements (SLAs)

Include cybersecurity requirements in SLAs with vendors, specifying security controls, incident response expectations, and data protection measures.

## 10. Business Continuity and Disaster Recovery

### 10.1 Business Continuity Plan (BCP)

Outline procedures to maintain critical university services during disruptions, including alternative work arrangements and communication strategies.

### 10.2 Disaster Recovery Plan (DRP)

Develop and test a disaster recovery plan to ensure that IT systems can be quickly restored after a major incident.

## 11. Continuous Improvement

### 11.1 Performance Metrics

Define key performance indicators (KPIs) to measure the effectiveness of cybersecurity measures, such as incident response times, user compliance rates, and vulnerability remediation timelines.

### 11.2 Framework Review

Review and update the cybersecurity governance framework annually or as needed to address emerging threats, changes in regulations, and lessons learned from incidents.

## 12. Communication Plan

### 12.1 Internal Communications

Establish protocols for communicating cybersecurity updates, incidents, and policy changes to faculty, staff, and students.

### 12.2 External Communications

Develop a communication strategy for public relations, including managing external inquiries and media engagement during security incidents.

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.

## 13. Related Documents/Policies

- Information Security Policy
- Access Control Policy
- Password Policy
- Electronic Messaging Policy
- Data Governance Policies