Alfaisal University

Policy Name:	Cyber Security Policy

Version #	**01**
Date Approved	
Effective Date	
Policy Owner	IT Services

Summary:

Alfaisal IT Services is committed to ensure appropriate security for information and IT systems in its domain of ownership. Furthermore, the university recognizes its responsibility to promote security awareness among the Alfaisal community. Failure to protect the university's information technology assets leads to financial, legal, and ethical implications.

The information in this document is subject to change without notice. No part of this policy may be reproduced for any purpose without the express written permission from Alfaisal University.

Table of Contents

1. Introduction

Alfaisal university is committed to safeguarding its information technology (IT) assets and ensuring the confidentiality, integrity, and availability of its data and systems. This cybersecurity policy establishes a framework for protecting its information systems and data from unauthorized access, use, disclosure, disruption, modification, or destruction.

2. Purpose

This policy establishes the cybersecurity requirements for the secure operation of Alfaisal University's information systems, ensuring the confidentiality, integrity, availability, and authorized use of digital resources. Policy Statement

- **Data Integrity**: Ensure data accuracy and completeness.
- **Data Confidentiality**: Protect the privacy and confidentiality of all university data.
- **Data Availability**: Ensure timely and reliable access to information systems and data by authorized users.
- **Accountability**: Track and log user activity to identify and address security incidents. Prevent users from denying their actions.
- **Authentication**: Verify the identity of users and devices accessing university systems.
- **Access Control**: Define and enforce roles and responsibilities related to cybersecurity.
- **Compliance**: Ensure compliance with all relevant legal, regulatory, and contractual obligations.
- **Awareness**: Promote cybersecurity awareness among all members of the university community.

3. Policy Scope

This Policy applies to all users accessing Alfaisal University's IT resources, including:

- **All users:** Faculty, staff, students, contractors, and third-party service providers.
- **All IT resources:** Servers, desktops, laptops, mobile devices, cloud services, network infrastructure (wired & wireless), IoT devices, and all university-owned, leased, or managed IT systems and data.
- **All access methods:** On-campus and remote access to university networks and systems.

4. Policy

Introduction/Purpose (Implied - No explicit section, but this is the overall purpose)

This policy establishes the cybersecurity framework for the University, outlining responsibilities, controls, and procedures to protect information assets and IT resources.

4.1.1. Risk Management

- Risk Assessment: The University will conduct periodic risk assessments to identify threats and vulnerabilities, prioritize risks, and determine appropriate mitigation strategies. These assessments will:
- Be conducted periodically, especially when business processes or technologies change.
- Require support from senior management and involve functional experts and IT staff.
- Be documented for audit and future reference.

4.1.2. Cybersecurity Controls and Procedures

Access Control: Access to University IT resources is restricted to authorized users only.

4.1.3. Data Protection:

- Sensitive and confidential data must be encrypted in transit and at rest.
- Regular data backups must be conducted and securely stored.
- Data retention and disposal must comply with legal and regulatory requirements.

4.1.4. Network Security:

- Firewalls, intrusion detection/prevention systems (IDS/IPS), and antivirus software must be deployed and maintained.
- Regular vulnerability assessments and penetration testing must be conducted.
- Network access must be segmented to limit exposure to critical systems.

4.1.5. Incident Response:

- The University will maintain a Cybersecurity Incident Response Plan.
- All security incidents must be reported immediately to the IT Security Team.
- Incident response procedures include detection, containment, eradication, recovery, and post-incident analysis.

4.1.6. Cybersecurity Controls: The University employs cybersecurity measures to:

- Protect data privacy.
- Prevent unauthorized system access.
- Prevent unauthorized data modification.
- Prevent unauthorized data dissemination.
- Defend systems against denial-of-service attacks.

Security Awareness and Training

4.1.7. Training and Awareness:

- All users must complete mandatory cybersecurity awareness training annually.
- Regular updates on emerging threats and best practices will be shared.
- Ongoing security awareness campaigns will educate users about common threats and best practices.
- Security information will be disseminated through various channels (e.g., email, newsletters, website).

4.1.8. Third-Party Risk Management

- Third-party service providers must comply with the University's cybersecurity standards.
- Contracts must include cybersecurity requirements and data protection clauses.

4.1.9. Compliance and Auditing

- Regular audits will be conducted to ensure adherence to this policy.
- Non-compliance may result in disciplinary action (e.g., termination of access, academic penalties, legal action).
-

5. Roles and Responsibilities

- Develop and maintain a comprehensive cybersecurity program.
- Provide adequate resources for cybersecurity initiatives.
- Conduct regular security assessments and risk management activities.
- Implement and enforce security controls and best practices.

- Provide cybersecurity training and awareness programs.
- Investigate and respond to security incidents.
- IT Security Team: Responsible for implementing and managing cybersecurity controls, monitoring security incidents, and responding to threats.
- Department Heads: Ensure departmental compliance with cybersecurity policies and practices.
- All Users (Faculty, Staff, and Students):
- Comply with all university cybersecurity policies and procedures.
- Use strong and unique passwords.
- Protect devices from unauthorized access.
- Report any suspicious activity or security incidents immediately.
- Use university resources responsibly and ethically.

6. University Rights and Non-Liability

The University reserves the right to:

- Restrict or disable accounts or access to IT resources to protect system integrity.
- Suspend accounts or access when policy or legal violations are suspected.
- Inspect and audit system configurations for compliance.
- Enforce this policy without prior notice.
- Conduct routine security scans of all connected devices to detect vulnerabilities and policy violations.

The University is not liable for personal content hosted on University resources or on personally owned devices connected to the University network.

7. Exemptions

Exception to or exemptions from any provision of this policy must be approved by the VPFA. Similarly, any questions about the contents of this policy, or the applicability of this policy to a particular situation should be referred to the IT Director.

8. Enforcement

Non-compliance with this policy could severely impact the operation of the institution by exposing the University to permanent loss of University data leading to loss of financial records, students' records, other records, research material. It may also expose the individual or the University to legal action.

9. Education

All Students, Staff and Faculty members shall be trained to know about their roles in creating a secure IT environment. Building awareness of IT security is an important element in establishing an environment in which each individual feels both responsible and empowered to act in their own and the community's best interests.

10. Definitions

Confidentiality Provides protection of information from either intentional or accidental attempts to access personal or university information by unauthorized entities.

Integrity Requires protection against either intentional or accidental attempts by unauthorized entities to alter data or modify information systems.

Availability Availability ensures timely and reliable access to and use of data and information technology resources to carry on the mission of the university.

Risk A source of danger; a possibility of incurring loss or damage. In general, risk is a composite of three factors: threats, vulnerabilities, and impact.

Risk factors Factors used to determine the level of risk include the effect of the loss on the university's strategic missions; the extent of loss to major information systems

Security incident An accidental or malicious act that exercises a vulnerability resulting in the potential of a negative impact.

Security The state of being free from unacceptable risk. IT security focuses on reducing the risk of computing systems, communications systems, and information being misused, destroyed, or modified, or for information to be disclosed inappropriately either by intent or accident.

Threats

Actions or events that potentially compromise the confidentiality, integrity, availability, or authorized use. These threats may be human or non-human, natural, accidental, or deliberate. Examples:

- Acts of malice by individuals or groups; purposeful or malicious use of information or information systems.
- Natural or physical disasters such as fire, flood, hardware failures.
- Unintentional oversight, action, or inaction; data left open to unauthorized access; accidental deletion of data files; inadequate data backup procedures.

Vulnerabilities

In computer security, vulnerability is a weakness which allows an attacker to reduce a system's assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. To be vulnerable, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the attack surface.

Examples:

- Software or hardware that allows unauthorized access to information systems.
- Business practices such as collecting and storing personal information that could, if revealed, be damaging to individuals.
- Personal practices or procedures such as improperly protecting one's password or providing inadequate physical environments for IT systems.