Alfaisal University

Policy Name:	Security & Information System Privacy 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.

Signature: ……..

Table of Contents

1. Introduction

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.

2. Purpose

This document outlines the university's policy for use and the requirements for adequate security for the university computers and network resources & safeguarding the confidentiality, integrity, availability and authorized Usage of the information systems.

3. Policy Scope

This policy applies to all users of the computer equipment owned, supplied or maintained by the university including servers, desktop computers, laptops, portable computers and those remote users connected to Alfaisal university network (servers and network resources).

4. Policy

4.1. General

4.1.1. Adequate security shall include the following:

A. Protection of the privacy of information.
B. Protection of systems against unauthorized access.
C. Protection of information against unauthorized modification.
D. Protection against dissemination of data in any form and,
E. Protection of systems against denial of service.

4.1.2. University computer and network resources may be accessed or used only by authorized individuals.

4.1.3. The university reserves the right at its sole discretion for the following

A. To restrict or disable any account or use of computer and network resources, and to inspect, copy, remove or alter any data, file, or system resources which may undermine authorized use in order to protect the security and integrity of computer and network resources.

B. The university reserves the right to suspend network access or computer account, as defined in this policy if user-maintained files, programs or services are believed to have been operating in violation of either law or policy.

C. To inspect or check the configuration of computer and network resources for compliance with this policy and to take appropriate actions it deems necessary to protect university computer and network resources.

D. The university can apply the provisions of this policy and the rights reserved to the university without prior notice to the user.

4.1.4. The university is not responsible for the content of users' personal web spaces, nor the content of programs or files that users maintain either in their personal allocated file areas on university-owned computer resources or on personally-owned computers connected to the university computer and network resources.

4.1.5. IT Services reserves the rights to conduct periodic scans of the university servers, computers and network resources (which include but no limited to personally-owned computers connected to the university's computer and network resources) for common security vulnerabilities, violations of policy or law.

5. Risk Assessment

Risk assessment is useful tool to recognize threats and vulnerabilities, the greatest risks are exposed and appropriate decisions are made regarding the risks to assume and those to mitigate through security controls.

The following factors will monitor the process to insure a successful risk assessment program:

A. Conducting a risk assessment periodically. As business processes or technologies change, periodic assessments must be conducted to analyze these changes, to account for new threats and vulnerabilities created by these changes, and to determine the effectiveness of existing controls.
B. Successful risk assessments require complete support of senior management and must be conducted by teams that include both functional experts and ITS Staff.
C. Documentation of risk assessments and resulting actions will be recorded for audit and future references.

6. Reporting of Security Incidents (All Users)

It is ethical responsibility of one and all to report security breaches or other security-related incidents. A critical factor of security is to address security breaches promptly.

Individuals aware of any breach of information or network security, or compromise of computer or network security safeguards, must report such situations to the IT Services Staff or the IT Director immediately.

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.