Princess Sumaya University for Technology

Risk Assessment

Princess Sumaya جامعـــة
University الأميـــرة سميّـــة
for Technology للتكنولوجيا

Anas Ereiqat

20200231

Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	1/31/2024		Document First Created

Document Contents Page

Document Version Control 2
Document Contents Page 3
Purpose 4
Scope 4
Information Security Policy 4
Principle 4
Introduction 4
Definitions 5
Information Security Objectives 5
Information Security Framework 5
Roles and Responsibilities 6
Review 7
Training and awareness 7
Compliance 7

Purpose

The purpose of the Information Security Policy is to:

- Protect CyberGuard's information assets from unauthorized access, alteration, or damage.
- Ensure the confidentiality, integrity, and availability of sensitive information.
- Define procedures to maintain the confidentiality, integrity, and availability of information technology resources.
- Protect CyberGuard's reputation and ensure compliance with legal and industry standards.

Scope

This policy applies to:

- Management of information security concerns at CyberGuard.
- All information systems and assets owned or accessed by CyberGuard.
- All users with access to CyberGuard's information systems and assets.
- Asset owners responsible for the assets they own.

Information Security Policy

Principle

- All users are responsible for information security.
- Divisions operating information systems must allocate duties for overseeing information security.
- External providers must comply with this policy.
- Information security is governed by a comprehensive framework.
- Internal audits are conducted regularly to assess the effectiveness of the information security program.
- Information security risks are managed using a risk-based approach aligned with CyberGuard's Risk Management Policy.

Introduction

The importance of information security in CyberGuard cannot be underestimated. It is critical to take the necessary steps to protect our critical and sensitive assets from data breaches and unauthorized access. Consequently, this policy, along with supplementary controls, are implemented to ensure protection of assets from internal and external factors.

Definitions

- Identify, manage, and treat information risks.
- Secure access and exchange of information.
- Meet compliance and legal obligations.
- Ensure users are trained and aware of their information security responsibilities.

Information Security Objectives

CyberGuard's information security objectives are to ensure:

- Identify, manage, and treat information risks.
- Secure access and exchange of information.
- Meet compliance and legal obligations.
- Ensure users are trained and aware of their information security responsibilities.

Information Security Framework

- Implement an Information Security Management System based on ISO 27001.
- Adopt a risk-based approach to controls, including encryption, acceptable use, backup, and others.

The enterprise will adopt a risk-based approach to the application of controls:

1. Acceptable Encryption Policy
2. Acceptable Use Policy
3. Backup Policy
4. Clean Desk Policy
5. Data Breach Response Policy
6. Email Retention Policy
7. Employee Internet Use Monitoring and Filtering Policy
8. End User Encryption Key Protection Policy
9. Internet usage Policy
10. Lab Security Policy
11. Password Construction Guidelines
12. Password Protection Policy
13. Remote Access Policy
14. Removable Media Policy
15. Risk Assessment Policy
16. Security Response Plan Policy
17. Software Installation Policy

Roles and Responsibilities

Department Heads/Managers/Supervisors

- Ensure the implementation of the information security policy across their departments at CyberGuard.
- Ensure employees' access to data is in compliance with regulations set forth by CyberGuard.
- Regularly review and document employees' access to data.
- Identify necessary information security training for employees.
- Provide approved resources and methods for securing equipment at CyberGuard.
- Report any inappropriate or illegal behavior to the designated information security officer.

IT Specialist

Provide technical support within CyberGuard's campus.

- Network Security Administrator
  Implement security controls and methods for information systems containing CyberGuard's data.
- Plan and implement security strategies for data transmission and storage at CyberGuard.
- Report possible security infringements or breaches at CyberGuard.
- Provide technical guidelines and training related to security at CyberGuard.

- Information Security Office
  Identify and treat internal and external risks to the confidentiality, integrity, and availability of information at CyberGuard.
- Develop and maintain security policies, plans, and strategies consistent with CyberGuard's policies.
- Ensure proper communication with internal and external audit teams at CyberGuard.
- Conduct regular reviews on security policies for compliance with standards and regulations at CyberGuard.
- Plan the financial budget for implementing security controls at CyberGuard.
- Conduct adequate training for all users on information system security at CyberGuard.
- Promote good security practices through awareness campaigns at CyberGuard.
- Develop a proper reporting platform for users to notify security infringements or breaches at CyberGuard.

Internal Audit

- Evaluate the effectiveness of current security measures and controls at CyberGuard.
- Provide recommendations on security measures for the information security office at CyberGuard.
- Perform regular and random audits as necessary at CyberGuard.

Users, including faculty, staff, and students

- Do not reveal or share sensitive information with unauthorized parties at CyberGuard.
- Do not alter CyberGuard's data without authorization.
- Access and store data in a secure manner at CyberGuard.
- Complete required information security training at CyberGuard.
- Sign a confidentiality agreement before accessing sensitive information at CyberGuard.
- Report any suspicious or inappropriate behavior to the Information Security Office at CyberGuard.

Review

- Conduct annual reviews of the policy.
- Obtain approval from the Board of Directors and Executive Group.

Training and awareness

- Promote understanding and compliance with policies and regulations.
- Address information security risks and physical security measures.
- Communicate consequences of non-compliance.

Compliance

- Supervise compliance with the policy.
- Enforce disciplinary and legal procedures for violations.
- Arbitrate violations on a case-by-case basis.