INSPIRING BUSINESS INNOVATION

جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY
عمادة الاتصالات وتقنية المعلومات
Deanship of Information and Communication Technology

Information Security Incident Management Policy

Version: 2.0

Policy Code: DICT-QAP012

Table of Contents

Table of Contents 2
Property Information 3
Document Control 4
Information 4
Revision History 4
Distribution List 4
Approval 4
Introduction 5
1. Policy Overview 6
1.1. Purpose 6
1.2. Scope 6
1.3. Terms and Definitions 6
1.4. Change, Review and Update 7
1.5. Enforcement / Compliance 8
1.6. Waiver 8
1.7. Roles and Responsibilities (RACI Matrix) 8
1.8. Relevant Documents 9
1.9. Ownership 10
2. Policy Statements 11
2.1. Responsibilities and Procedures 11
2.2. Reporting Information Security Events 12
2.3. Reporting Information Security Weaknesses 13
2.4. Assessment of and Decision on Information Security Events 14
2.5. Response to Information Security Incidents 14
2.6. Proactive information about threats 16
2.7. Learning from Information Security Incidents 16
2.8. Collection of Evidence 17

Property Information

This document is the property information of Imam Abdulrahman bin Faisal University - ICT Deanship. The content of this document is intended only for the valid recipients. This document is not to be distributed, disclosed, published or copied without ICT Deanship written permission.

Document Control

Information

Title	Classification	Version	Status
Information Security Incident Management Policy	High	2.0	validated

Revision History

Version	Author(s)	Issue Date	Changes
0.1	Alaa Alaiwah - Devoteam	09 November 2014	Creation
0.2	Nabeel Albahbooh - Devoteam	1 December 2014	Update
1.0	Nabeel Albahbooh - Devoteam	31 December 2014	Update
1.1	Muneeb Ahmad – ICT, IAU	27 April 2017	Update
1.2	Lamia Abdullah Aljafari	6 June 2020	Update
2.0	Dr. Bashar AlDeeb	22 Sept 2020	Update
2.0	Manal Mohamed Alhejazi	17 March 2021	Update
2.1	Mohammad Younes	22 March 2022	Update

Distribution List

#	Recipients
1	Legal Affairs
2	Website
3	Quality Assurance Department - DICT

Approval

Name	Title	Date	Signature
Dr. Khalid Adnan Alissa	Dean of DICT	30-6-2022	

Introduction

The purpose of this policy is to provide cybersecurity requirements based on IAU's best practices and standards related to cybersecurity incident and threat management to reduce and protect cyber risks from internal and external threats by focusing on the primary protection objectives: confidentiality, integrity, and availability of information.

This policy aims to comply with cybersecurity requirements and related legislative and regulatory requirements

This policy covers all information and technology assets of the IAU.

The information assets' confidentiality, integrity and availability are essential to maintain University of Imam Abdulrahman bin Faisal security compliance.

1. Policy Overview

This section describes and details the purpose, scope, terms and definitions, change, review and update, enforcement / compliance, wavier, roles and responsibilities, relevant documents and ownership.

1.1. Purpose

The main purpose of the **Information Security Incident Management Policy** is to:

Ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

1.2. Scope

The policy statements written in this document are applicable to all IAU's resources at all levels of sensitivity; including:

- All full-time, part-time and temporary staff employed by, or working for or on behalf of IAU.
- Students studying at IAU.
- Contractors and consultants working for or on behalf of IAU.
- All other individuals and groups who have been granted access to IAU's ICT systems and information.

This policy covers all information assets defined in *Risk Assessment Scope Document* and will be used as a foundation for information security management.

1.3. Terms and Definitions

Table 11 provides definitions of the common terms used in this document.

Term	Definition
Accountability	A security principle indicating that individuals shall be able to be identified and to be held responsible for their actions.
Asset	Information that has value to the organization such as forms, media, networks, hardware, software and information system.
Availability	The state of an asset or a service of being accessible and usable upon demand by an authorized entity.
Confidentiality	An asset or a service is not made available or disclosed to unauthorized individuals, entities or processes.

Control	A means of managing risk, including policies, procedures, and guidelines which can be of administrative, technical, management or legal nature.
Guideline	A description that clarifies what shall be done and how, to achieve the objectives set out in policies.
Information Security	The preservation of confidentiality, integrity, and availability of information. Additionally, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.
Integrity	Maintaining and assuring the accuracy and consistency of asset over its entire life-cycle.
Owner	A person or group of people who have been identified by Management as having responsibility for the maintenance of the confidentiality, availability and integrity of an asset. The Owner may change during the lifecycle of the asset.
Policy	A plan of action to guide decisions and actions. The policy process includes the identification of different alternatives such as programs or spending priorities, and choosing among them on the basis of the impact they will have.
Risk	A combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.
Supplier	A party that provides equipment or services.
System	An equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, control, display, switching, interchange, transmission or reception of data and that includes computer software, firmware and hardware.

Table 1: Terms and Definitions

1.4. Change, Review and Update

This policy shall be reviewed **once every year** unless the owner considers an earlier review necessary to ensure that the policy remains current. Changes of this policy shall be exclusively performed by the Information Security Officer and approved by Management. A change log shall be kept current and be updated as soon as any change has been made.

1.5. Enforcement / Compliance

Compliance with this policy is **mandatory** and it is to be reviewed periodically by the Information Security Officer. All IAU units (Deanship, Department, College, Section and Center) shall ensure continuous compliance monitoring within their area.

In case of ignoring or infringing the information security directives, IAU's environment could be harmed (e.g., loss of trust and reputation, operational disruptions or legal violations), and the fallible persons will be made responsible resulting in disciplinary or corrective actions (e.g., dismissal) and could face legal investigations.

A correct and fair treatment of employees who are under suspicion of violating security directives (e.g., disciplinary action) has to be ensured. For the treatment of policy violations, Management and Human Resources Department have to be informed and deal with the handling of policy violations.

1.6. Waiver

Information security shall consider exceptions on an individual basis. For an exception to be approved, a business case outlining the logic behind the request shall accompany the request. Exceptions to the policy compliance requirement shall be authorized by the Information Security Officer and approved by the ICT Deanship. Each waiver request shall include justification and benefits attributed to the waiver.

The policy waiver period has maximum period of 4 months, and shall be reassessed and re-approved, if necessary for maximum three consecutive terms. No policy shall be provided waiver for more than three consecutive terms.

1.7. Roles and Responsibilities (RACI Matrix)

Table 2 shows the RACI matrix[1] that identifies who is responsible, accountable, consulted or informed for every task that needs to be performed.

There are a couple of roles involved in this policy respectively: Management, ICT Deanship, Information Security Officer (ISO), Legal Department and User (Employee and Contractor).

[1] The responsibility assignment RACI matrix describes the participation by various roles in completing tasks for a business process. It is especially useful in clarifying roles and responsibilities in cross-functional/departmental processes. R stands for Responsible who performs a task, A stands for Accountable (or Approver) who sings off (approves) on a task that a responsible performs, C stands for Consulted (or Consul) who provide opinions, and I stands for Informed who is kept up-to-date on task progress.

Roles / Responsibilities	Mgt.	ICT	ISDept	Legal	User
Establishing security incident management framework.	I	R,C	R,A		I
Developing and reviewing the processes, framework, policy and procedures for incident management.	I	R,C	R,A		I
Developing and reviewing the guidelines for incident handling and classification.	I	R,C	R,A		I
Identifying, documenting and maintaining rules for collection, retention and presentation of information security incident evidences.	I	R,C	R,A		I
Coordinating a response to actual or suspected breaches in the confidentiality, integrity or availability of critical IAU's business information.	I	R,A	R,C		
Investigating breaches of security controls, and implementing additional compensating controls when necessary.	I	R,A	R,C		
Managing the response to an incident and ensuring that all procedures are correctly followed.	I	R,A	R,C		
Reviewing incidents to determine what lessons can be learnt and what process improvement may be required.	I	R,A	R,C		
Reviewing and recommending technologies to manage and respond to any possible incidents.	I	R,A	R,C		
Reporting to Management any serious incidents that may require a critical decision.	I	R,A	R,C		
Providing the expert legal advice that is necessary for other departments to provide services in a manner that is fully compliant with existing laws and regulations.		C	C	R,A	I
Adhering to information security policies, guidelines and procedures pertaining to the protection of information.		C	C		R,A,I
Reporting actual or suspected security incidents to ICT Deanship.	I	C	C		R,A,I

Table 2: Assigned Roles and Responsibilities based on RACI Matrix

1.8. Relevant Documents

The followings are all relevant policies and procedures to this policy:

- Information Security Policy
- Human Resource Security Policy
- Asset Management Policy
- Access Control Policy
- Information Security Aspects of Business Continuity Management Policy
- Compliance Policy
- Risk Management Procedure
- Incident Response Procedure
- Service Desk Rules and Escalation Policy

1.9. Ownership

This document is owned and maintained by the ICT Deanship of Imam Abdulrahman Bin Faisal University.

2. Policy Statements

The following subsections present the policy statements in 7 main aspects:

- Responsibilities and Procedures
- Reporting Information Security Events
- Reporting Information Security Weaknesses
- Assessment of and Decision on Information Security Events
- Response to Information Security Incidents
- Learning from Information Security Incidents
- Collection of Evidence

2.1. Responsibilities and Procedures

1. Information security incidents responsibilities and appropriate procedures shall be established to ensure an effective response against information security related events.
2. All IAU's employees shall understand their responsibility towards reporting related security incidents.
3. Information Security Officer in cooperation with ICT Deanship shall develop an information security incident management process. This process shall include, but not be limited to:
    a. Identification of the incident, analysis to ascertain its cause and vulnerabilities it exploited.
    b. Limiting or restricting further impact of the incident.
    c. Monitoring and reporting the incident.
    d. Tactics for containing the incident.
    e. Responding and escalating the incident.
    f. Corrective action to repair and prevent reoccurrence.
    g. Communication across IAU to those affected.
    h. Collection of any evidence.

4. ICT Deanship shall deploy, where possible, a monitoring control system to detect any information security incidents.
5. Information related to information security incidents shall never be communicated to third parties (e.g., public, journalists, etc.).
6. All information security incidents resulting in disruption in the services or loss of assets shall be analyzed to identify any emerging trends. All such incidents and trend analysis shall be reported to Information Security Officer and ICT Deanship in a periodic basis.
7. Potential information security incidents shall be communicated to relevant personnel who shall assist in corrective actions to be taken.

REF: [ISO/IEC 27001: A.16.1.1]

2.2. Reporting Information Security Events

1. Information Security Officer in cooperation with ICT Deanship shall develop an "Information Security Incident Management Form" in order to report all security violations/incidents which establish a quick response mechanism to information security incidents.
2. All IAU's employees shall understand, and be able to identify any unexpected or unusual behavior on the assets which could be a potentially software malfunction. Security events may include, but not be limited to:
    a. Uncontrolled system changes.
    b. Access violations (e.g., password sharing).
    c. Breaches of physical security.
    d. Systems being hacked or manipulated.
    e. Loss of information confidentiality (e.g., data theft).
    f. Compromise of information integrity (i.e., damage to data or unauthorized modification).
    g. Misuse of information, assets and or services.
    h. Systems infection by unauthorized or harmful program and or software.
    i. Unauthorized access attempt.
    j. Unauthorized changes to hardware, software or infrastructure configuration.

k. Unusual system behavior.

3. If a security event is detected, users shall perform the following:
    a. Note the symptoms and any error messages on screen.
    b. Disconnect the workstation from the network if an infection is suspected (with assistance from ICT Deanship).
    c. Not use any removable media (e.g., USB memory sticks) that may also have been infected.
4. All IAU's employees shall immediately report all suspected security related events to ICT Deanship. The following information shall be supplied, but not be limited to:
    a. Contact name and number of people reporting the incident.
    b. The type of information or equipment involved.
    c. Whether the loss of the information puts any person or other data at risk.
    d. Location of the incident.
    e. Inventory numbers of any equipment affected.
    f. Date and time the security incident occurred.
    g. Location of data or equipment affected.
    h. Type and circumstances of the incident.
5. ICT Deanship shall generate reports on incidents on a monthly basis and consolidate into the ITC Service Report every quarter.
6. The National Cybersecurity Authority must be reported on cyber security incidents.
7. The IAU shall inform the National Cybersecurity Authority of incident notifications, indicators and reports of violations.

REF: [ISO/IEC 27001: A.16.1.2]

2.3. Reporting Information Security Weaknesses

1. All IAU's employees shall report any suspected information security related weaknesses in systems or services.

2. Information security related weaknesses shall be reported to ICT Deanship as quickly as possible and the incident response and escalation procedure shall be followed. Security weaknesses may include, but not be limited to:

   a. Inadequate firewall or antivirus protection.

   b. System malfunctions or overloads.

   c. Malfunctions of software applications.

   d. Human errors.

REF: [ISO/IEC 27001: A.16.1.3]

2.4. Assessment of and Decision on Information Security Events

1. ICT Deanship shall evaluate an information security incident in terms of criticality, based on the existing or possible business impact as per the following scheme:

		Urgency		
		High	Medium	Low
Impact	High	1	2	3
	Medium	2	3	4
	Low	3	4	5

2. All information relevant to security incidents shall be classified based on the existing incident classification scheme. ICT Deanship shall be responsible for assigning the appropriate classification level to each security incident with Management approval.

REF:[ISO/IEC 27001: A.16.1.4]

2.5. Response to Information Security Incidents

1. ICT Deanship shall adopt a formal "Information Security Incident Management Procedure" which defines the required steps to be taken in response to any information security related incident.

2. The response to an incident shall be logged as per the following scheme:

Priority	Definition	Target Response	Target Resolution
1	Major Incident	10 minutes	4 hours
2	High	30 minutes	8 hours

Priority	Definition	Target Response	Target Resolution
3	Medium	1 hour	2 days
4	Low	4 hours	5 days
5	Planning	2 days	10 days

3. The actions required to recover from the information security incident shall be under a formal control. Only identified and authorized employees shall have access to the affected systems during the incident; and all of the remedial actions shall be documented as much detail as possible.

4. The procedures for recovering from cybersecurity incidents should include identifying the exploits that were exploited during the incident and addressing them with the necessary technical and administrative measures, for example:

    - Implementation of Compensating Controls.
    - Installing the updated patches and updates.
    - Restore system backups.
    - Resetting the security systems settings, such as the firewall and intrusion detection systems.

5. ICT Deanship shall be responsible to keep a track of status of incident by following up with relevant parties or persons and handling queries related to status of incident. All information security incidents shall be recorded and allocated an incident number for tracking and future reference. The record may include, but not be limited to:

    a. Causes: whether direct and indirect, this led to the incident to happen.

    b. Impact: which systems suffered during the incident.

    c. Actions taken: by the user and ICT Deanship employees to report and manage the incident.

    d. Level of damage: what were the losses caused.

    e. Date and time of occurrence.

6. The incident response procedure shall be a seamless continuation of the event reporting process and shall include contingency plans to ensure the continuing operation of information systems during the incident.

REF:[ISO/IEC 27001: A.16.1.5]

2.6. Proactive information about threats

1. It is necessary to engage with providers of proactive information (Threat Intelligence) to keep abreast of incidents and threats related to cyber security and to deal with that information directly.

2. Proactive information on threats should be saved and organized in a flexible and convenient database for formulating action notes and indicator metadata, such as the Knowledge Base.

3. Intrusion Prevention and Detection Systems must be updated with proactive threat information and ensure that these systems can detect and deal with threats effectively.

2.7. Learning from Information Security Incidents

1. ICT Deanship shall collate and review the post incident information on a regular basis. Any changes to the process made as a result of the post incident review shall be formally noted.

2. After each incident, a lessons-learned exercise shall be conducted by ICT Deanship; shall be analyzed; and the results shall be adequately documented. The followings shall be considered:

    a. Conducting post incident analysis in a timely manner to determine the damage/cost incurred, confirm the cause, motive of the attack and any potential mitigating actions.

b. Performing an assessment of the involved systems to ensure that no additional user accounts have been created and user privileges have not been modified during incident response.

REF: [ISO/IEC 27001: A.16.1.6]

2.8. Collection of Evidence

1. Information Security Officer in cooperation with ICT Deanship shall identify, document and maintain rules for collection, retention and presentation of evidence based on IAU's security, regularity and legal requirements.
2. If an incident may require information to be collected for an investigation strict; rules shall be adhered to. The collection of evidence for a potential investigation shall be approached with care. The followings shall be considered:
    a. Whenever evidence clearly shows that IAU has been subject to a computer or communications crime, a thorough investigation shall be performed.
    b. This investigation shall provide sufficient information to assist management with re-establishing security measures and preventing the reoccurrence of such incident.
3. Information Security Officer shall be contacted immediately for guidance; and strict processes shall be followed for the collection of forensic evidence such as digital evidence, physical evidence, original evidence and copies of evidence.

REF:[ISO/IEC 27001: A.16.1.7]

---------- End of Document ----------