جـامعـة الشـارقـة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Information Security Incident Management	Last Review date	10/05/2024
	Policy Number	ITC-21	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs

Overview

This document establishes a process requirement that help manage and control the IT security incidents of the University of Sharjah information and information processing facilities. It is intended to protect the security of UOS data and technology infrastructure.

Scope

The scope of this policy covers all users at the university of Sharjah accessing and using data and information system in all the locations.

Purpose

The purpose of the University of Sharjah Information Security Incident Policy is to :

- provide users with information on Information Security Incident management processes.
- Ensure protection of the University of Sharjah's information and information assets.

Policy

- All information security Incident shall be reported in the "ITC Service desk" or to the information security team.
- IT Help Desk Email: IT Service Desk servicedesk@sharjah.ac.ae
- The channels of communication shall be, but not limited to:
    a. Emails
    b. Oral Communication to the Concerned team
    c. Phone Calls
- All employees and non-employees of the University of Sharjah shall be made aware of their responsibilities on communicating information security incidents and the channel of communication.
- Helpdesk team shall make necessary evaluation to ensure that the incident "to be recorded" is an actual information security incident and that it requires information security team attention.
- All information security incidents reported shall have at a minimum the following details captured:
    a. Category of the information security incident.
    b. Details of the user(s) who reported the information security incident
    c. Information security incident description
    d. Date and time Identified
    e. Department/ Section where the information security incident identified

Procedures

Management of information security incidents

Information security incident management consists of the following five distinct phases which must be catered correctly:

Plan and prepare

1. The information security team shall assist in carrying out information security incident response activities.
2. The information security team will handle information security incident with high and medium priorities
3. Each information security incident shall be classified based on the priority and the areas of impact, as follows:
    a. Critical: information security incidents that have an immense impact on the university of Sharjah business or service
    b. High: information security incidents that have some detrimental impact on the University of Sharjah and require immediate investigative or mitigating action.
    c. Medium: information security incident of medium significance requiring investigation or mitigation, but not urgent.
    d. Low: Insignificant impact requiring little or no investigation or remediation.

4. The university of Sharjah shall deploy an information security incident management software systems to:
    a. Collect consistent and time sensitive information related to information security incidents.
    b. Automate the approval process of an information security incident report or case investigation.
    c. Collect real time information security incident information such as time and date data.
5. Information security Incident event management system (SIEM) or team will send notifications; assign tasks and escalations to appropriate individuals depending on the information security incident type, priority, time, and status and custom criteria.
6. Information security incident management software will send notifications to the parties involved in opening, maintaining, and closing the information security incident ticket.
7. Management reports produced from this system shall provide a summary of all information security incidents and the collection of information security incidents based on geography, type of users, departments, dates and other data fields provided in the system.

Detection and reporting

1. All information security incidents shall have relevant information collected to analyze the Information security incidents and identify root cause of the information security incident.
2. Information Security incident shall be categorized as follows:
    a. Access Violation
    b. Accidental Incidents
    c. Environmental
    d. Inappropriate Use
    e. Malicious Incident
    f. Operational
3. "IT helpdesk" shall act as first point of contact for all concerned users until information security incident closure.
4. All information security incidents shall be treated as confidential.
5. Information Security Team shall have the authority to prioritize the information security incidents based on the impact and the analysis conducted.
6. Respective team shall be identified and the information security incident shall be allocated accordingly.
7. Perpetrators of Cyber Crime shall be handled fully based on the law.

Assessment and decision

1. The information security team shall be responsible to perform first line of assessment of the information security incident with high and medium priority and to reprioritize the information security incident, if needed.
2. The information security team will perform root cause analysis, if required with appropriate vendors. The same shall be documented in the information security incident management system.
3. Non-disclosure agreement need to be signed with relevant vendors
4. The information security team will only handle computer/network related information security incidents which are classified as Medium, High or Critical.
5. The information security team shall brief the designated representatives from other departments.
6. Actions shall be taken to correct and close the information security incident.
7. The information security incident, if not contained and corrected within the pre-defined timeframes, shall be escalated to the next level of action.

Incident analysis and forensics

1. The audit trails and any similar evidence shall be collected and secured for post-incident analysis and for forensic analysis.
2. These evidences shall be used by the legal, HR department and the cyber security enforcement against users in the court of law based on the following laws:

a. Federal Law No. 1 of Year 2006 on Electronic Commerce and Transactions.
b. Federal Law No. 2 Year 2006 on the Prevention of Information Technology Crimes.

Responses

1. Root cause analysis will be conducted and accordingly corrective actions will be identified to ensure that the information security incident is properly closed.
2. All relevant stakeholders shall be updated about the information security incident.
3. The result of the analysis might lead to policies and security controls changes.

Lessons learnt

1. Information security team will receive training on information security incident management process as defined and required by the information security head.
2. A knowledge-based shall be maintained to record all information security incidents and to conduct root cause analysis.
3. Corrective actions and corrections subjected to the cause of information security incidents will be recorded in detail to ensure that resolution process is available if needed.
4. Analysis shall be done on the recorded information security incidents to understand the effectiveness of implemented security controls.
5. These learnings shall assist in decision-making and analysis for future information security incidents.

Reference

Standard	Control Ref
ISO 27001:2013	A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7,