جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology	Effective Date	30/5/2021
	Policy Subject	Third Party Security	Last Review date	19/5/2021
	Policy Number	IT-30	Next Review date	19/5/2022
	Responsible Entity	IT Center	Approved By	VC for Financial & Admin. Affairs

Overview

Third party services are needed to increase effectiveness, improve core services and costs, however it also increases the exposure to loss, theft and misuse of data. Risk management and information security controls must be in place to avoid such events

Scope

This policy is applicable to all systems, and information processing facilities as well as all third-party personnel who are using the University of Sharjah's information assets and systems.

Purpose

The purpose of this policy is to establish controls to ensure that access provided to Third Party is as per appropriate security practices and will not allow them to carry out any unauthorized activity. The policy also ensures that all third party service providers shall abide by and follow the information security requirements and practices set forth by UoS.

Abbreviations and Definitions

PII – Personally identifiable information
OWASP – Open Web Application Security Project
DR – Disaster recovery
SDLC – Systems development life cycle
NDA – Non disclosure agreement
SLA – Service level agreement
Third Party – An individual or organization that deals with the University of Sharjah through a business relationship and has access to university's information assets or information processing facilities.

Policy

Identification of Risks related to third parties

1. Risk assessment shall be conducted to identify potential risks to UOS Information Security as a result of third party access.
2. These risks shall be appropriately controlled through effective controls that need to be implemented to regulate and monitor the confidentiality, integrity and availability of the information processed by the third party.
3. All third-party access to UOS's Information Systems, LAN, WAN and wireless infrastructure shall have formal authorization as per data access policy.

4. Outsourcing of information or data processing functions or services to third parties shall be formally authorized by the Business Owner / ITC director. Signing of Underpin contract shall be a mandatory process before allowing access to the third-party users.
5. The Analysis of Risks related to Third Party access must consider:
    a. Possible Impacts to the controls of the information processing facilities involved
    b. The classification of the information assets
    c. Processes for identifying, authorizing, authenticating and reviewing access rights of the third party
    d. Security Controls to be used by the third party when storing, processing, communicating, sharing or exchanging information.
    e. Possible Impact to both parties resulting from assets being unavailable
6. ITC shall maintain the list of all third-party contractors or consultants. In event of any replacement of contractor or consultant the third party shall inform officially.
7. Prior to authorizing access to third parties to information and information systems Information Owners and Information Custodians must confirm that:
    a. The terms and conditions of access are documented (e.g. Service Level Agreement (SLA), Underpin Contracts, Memoranda of Understanding)
    b. Responsibilities for managing and monitoring the third party access have been assigned and documented
    c. Security Controls have been implemented and tested against identified risks.

Third Party Access Policy

1. All System access by third parties such as contractors, customers, consultants or other third staff must be based on underpin contract and Non-Disclosure Agreement (NDA).
2. Access to UOS Systems or other IT resources by Third parties must be restricted to the services and information they are explicitly authorized to access.
3. All Third parties & Customers shall be provided with a Separate User Account for access and this account shall expire on completion of the business requirement.
4. Third party requesting internet access shall accept ownership of account allocated and is responsible for all actions performed with the user Account.
5. The Third-Party account shall be disabled when not in use and password shall be managed as per UOS's Password Policy.
6. All Third-Party users utilizing UOS Internet connectivity shall abide by UOS Internet Policy.

7. Third-Party Personnel using his/her Personal Laptop in UoS networks must be checked to ensure it is updated with the latest Anti-Virus Software & definitions and free from hacking / cracking tools.
8. No third party shall be granted remote access unless prior approval and authorization is granted from the information security team.

Addressing Security in Third Party Agreements

1. Third party access to UOS's information systems shall be provided based on a formal contract between UOS and the third party.
2. Contracts with third parties, for provision of external parties with access to UOS's information systems shall be consistent in all respects with UOS's Information Security policies and procedures.
3. Agreements with any third party shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.
4. Outsourcing contracts shall be consistent in all respects with UOS's Security policies as well as other university policies existing at the time of contract.
5. Outsourcing contracts shall include the following conditions as a minimum: -
    a. The level of physical and logical security to be provided to the third party to maintain the confidentiality and integrity of UOS's information / data processed.
    b. The service level to be provided and the level of availability in the event of a disaster.
    c. Provision for confidentiality, non-disclosure and acceptable use relating to the information /data processed by the outsourced function or service.
6. UOS shall have the right to review and audit compliance with the terms of the outsourcing contract.

Reference

Sl No	Standard Name	Control Ref
1	ISO 27001:2013	A8.1.4, A.9.2.6, A.13.2.2