 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Supplier Management	Last Review date	10/05/2024
	Policy Number	ITC-28	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs

Overview

Suppliers management is the way of dealing with supplier and managing the daily communication with them. It includes but not limited to working collaboratively with suppliers, managing vendor deliverables and financial commitment (payments and installment). Protect any information assets or processing facilities belonging to the UoS to which third party supplier access (or potential access) is very crucial. Compliance with this Policy contributes to the University meeting its governance requirements.

Scope

This policy is covering all external parties, suppliers, vendors, and contractor of the University of Sharjah Information Technology Centre.

Purpose

The purpose of this policy is to define and implement the appropriate level of administrative and security measures while dealing with external vendors and contractors to protect information resources of the University of Sharjah.

Abbreviations and Definitions

NDA: Non-Disclosure Agreement


SLA: Services Level Agreement

ITC: Information Technology Center

UoS: University of Sharjah

Policy

- The Information Technology Centre shall follow the University of Sharjah tendering and procurement process.
- Due diligence shall be exercised while evaluating External Parties services to ensure accuracy of their claimed qualifications and successful delivery of contractual obligations.
- ITC in coordination with business Owner shall ensure that contractual agreements in terms of legal, business / academic and technical requirements are negotiated and agreed with the suppliers, before commencing the project.

 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Supplier Management	Last Review date	10/05/2024
	Policy Number	ITC-28	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs

Procedures

Identification of Risk Related to Suppliers

1. The Information Security Team, business owners and operations team shall ensure that the periodic information security risk assessment identifies potential Suppliers risks that could compromise the Confidentiality, Integrity & Availability of Information assets & information processing facilities.
2. Systems Administrator in coordination with Information Security and other relevant teams shall identify any additional security/operational risk specific to the project.
3. The analysis of risks related to supplier's access to information and information processing facilities shall consider the following:
 - a. Possible impacts to the controls of the information processing facilities.
 - b. The classification of the information assets.
 - c. Processes for identifying, authenticating, authorizing and reviewing access rights of the External Parties.
 - d. Security/operational controls that are in place to control storing, processing, communicating, sharing or exchanging information.
 - e. Training requirements for the university personnel involved in contractual relationship with the suppliers.
 - f. All risks identified shall be appropriately addressed through risks mitigation measures.
4. Wherever required, operational / security requirements and controls shall be documented in an agreement and signed by both the parties.


Non-Disclosure Agreement Sign-off

The IT / Business / academic /Projects Owners shall ensure that NDA (Non-Disclosure Agreement) is signed by any Supplier. The NDA shall be signed before commencing project/initiative or any service modification.

Supplier contracts and agreements

Based on the criticality of the project and the engagement, the below clauses can be considered as part of Supplier Contracts:

1. Compliance with legal and regulatory requirements.
2. Compliance with Intellectual property rights requirements.
3. Compliance with IT policies and procedures.
4. Compliance with procurement policies and procedures
5. Clear allocation of responsibilities to all the involved parties.
6. Statement on Non – Disclosure of information.
7. ITC rights to review and audit the compliance with the contracts.
8. Adequate Service Level Agreements (SLA), where applicable.
9. Details on the type and classification of information and method of providing access.
10. Relevant regulations for sub-contracting, including the controls that need to be implemented.
11. Supplier's obligations to comply with the university's security requirements.

 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Supplier Management	Last Review date	10/05/2024
	Policy Number	ITC-28	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs

Monitoring and Review of External Parties Services

Respective Systems administrator shall maintain appropriate reports and records, to monitor and measure the compliance with the ITC requirements. The Suppliers shall be responsible to take appropriate actions to address any non-conformity that might be identified during the compliance review.

Termination of External Parties Services

1. Proper transition and exit management provisions shall be considered to ensure correct procedures for handing over external contracts or services back to Sharjah University's ITC.
2. Operations team/Systems administrator shall ensure that proper transfer of knowledge is obtained from the Suppliers for the ongoing operation / maintenance.
3. Upon completion/termination of an engagement with Suppliers, the System administrator shall inform the relevant information assets owners/custodians to revoke the access rights of the Suppliers who were granted access to the information processing facilities.

Reference

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