 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	IT Service Management	Last Review date	10/05/2024
	Policy Number	ITC-22	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs

Overview

The University of Sharjah IT Service Management policy mandates the design, plan, delivery, operation and control technology services offered by UoS Information Technology Center.

Scope

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

Purpose

The purpose of this policy is to set forth the requirements for the University of Sharjah IT services management processes for managing the IT Services managed by ITC.

Abbreviations and Definitions

ITC: Information Technology Center.

UoS: University of Sharjah.


Policy

- The UoS's System administrator shall ensure that operating procedures and work instructions for information systems are Standardized.
- Access to the system should be restricted to only those who have a business need and are authorized.
- Access to the system shall be controlled using firewalls, in order to reduce the risk of accidental changes, configuration/data incompatibilities and unauthorized access.
- All systems shall be tested prior to deployment to production, in an appropriate test environment.
- Purchase of software, IT equipment and peripherals should follow a standard evaluation process.
- All software and hardware installations for the Departments shall be tested by UOS personnel, in test environment prior to being deployed to the production environment.
- Service owners shall monitor the capacity demands of UOS and make projections of future capacity requirements to ensure that cost justifiable capacity exists to meet requirements.

Procedures

Operations

1. System administrator shall ensure that operating procedures and work instructions for information systems and standards are:
 - a. Documented and controlled
 - b. Consistent with UOS Information Security Policies
 - c. Reviewed and updated periodically
 - d. Reviewed and updated post any changes to the infrastructure or services.
2. Documented operating procedures shall be communicated to the users as appropriate and jobs shall be carried in accordance with the operating procedure.

 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	IT Service Management	Last Review date	10/05/2024
	Policy Number	ITC-22	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs


3. System documentation should be kept under safe custody to protect against unauthorized access, modification and destruction. Respective custodians of documents shall hold the original set of System Documentation.
4. Access should be restricted to only those who have a business need and are authorized. Access to the confidential system documentation if any should be logged

Segregation of Development, Test and Operational Environments

1. Development and test environments shall be separated from live operational environments physically and logically and the access to each shall be mutually exclusive and controlled using firewalls, in order to reduce the risk of accidental changes, configuration/data incompatibilities and unauthorized access.
2. Transfer of software between the development, test and operational environments shall be subject to specific procedures and authorizations and will be documented
3. Operation environments shall be secured by:
 - a. Segregating production environment from test and development environments by using different servers, domains and partitions.
 - b. Preventing the use of test and development system identities and credentials for operational information systems.
 - c. Preventing access to compilers, editors and other tools in the operational information systems.
 - d. Using approved change and release management process for deploying and rollout of software/application from development/test to production.
 - e. Prohibiting the use of live operational data in development, test or training. When such use is necessitated, copies of the production data files will be made and sanitized and taken offline for that purpose. Those copies shall be handled carefully and purged when completed to prevent unauthorized exposure of production data. At all the times, system test data shall be segregated from the production data.

Service Acceptance

1. All systems shall be tested prior to deployment to production, in an appropriate test environment.
2. A system acceptance plan should be established to cover:
 - a. System performance requirements of the business
 - b. Security requirements of UOS.
 - c. UOS's business continuity requirements.
 - d. Error recovery and restart procedures.
 - e. Effects of the new system on other existing systems.
 - f. User / IT training and guides to ease of use of new systems, so as to ensure desired level of user performance.
 - g. As part of new service onboarding the system acceptance needs to be obtained from stakeholders through the relevant process.
 - h. Application governance document needs to be maintained

 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	IT Service Management	Last Review date	10/05/2024
	Policy Number	ITC-22	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs

- i. Backup Plan, Roll Back Plan and DR Plan.
 - j. Additional / Removal of services or changes in the SLAs.
3. The system should be sanitized (like removing the test users, dummy transactions and test data etc.) after satisfactory testing, before being moved to production environment.

Purchase and Installation of New IT Systems

1. Purchase of software, IT equipment and peripherals shall follow a standard evaluation process.
2. All software and hardware installations for the Departments shall be tested by UOS personnel, in test environment prior to being deployed to the production environment.
3. Any changes to software or hardware configuration shall follow the change management process.
4. Users shall not have administrator rights to their laptops and desktops which enables them to install software.

Capacity Management


1. Service owners shall monitor the capacity demands of UOS and make projections of future capacity requirements to ensure that cost justifiable capacity exists to meet requirements.
2. Service Owner shall establish and implement a formal process for capacity management. The process shall include following periodic activities:
 - a. Review and analysis of the resource utilization reports and trends
 - b. Review and analysis of the business plan covering on going and upcoming projects
 - c. The development of capacity plans to meet the current and projected demand for the capacity, power and reliability of systems and networks
 - d. Review of capacity plans
 - e. Appropriate load and stress testing must form an essential part of the testing plan and the acceptance criteria for new or upgraded enterprise applications

Segregation of Duties

1. UOS IT processes shall adopt the principle of segregation of duties. For e.g. personnel involved in operational functions shall not be given additional responsibilities in IT administration processes and vice versa.
2. The process shall include compensating controls wherever segregation of duties is not possible or practical such as monitoring of activities, maintenance and review of audit trails and management supervision.
3. The roles of testing and operational staff shall be segregated, and cross functional audits will be enforced to minimize the errors and misuses.

Server Management

1. All security-related service packs, patches, and hot-fixes shall be tested and applied to servers as per the Patch Management Process.
2. All servers shall be protected by antivirus software.

 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	IT Service Management	Last Review date	10/05/2024
	Policy Number	ITC-22	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs

3. Servers must not have direct internet access. All internet-access network attempts must be captured and monitored.
4. All servers' backups shall be as per the data backup policy.
5. Warning banners that specify requirements and penalties for accessing the system will be provided upon access to the server.
6. All non-essential services, users, group, and service accounts shall be removed.
7. Access to server consoles and operating systems shall always be through remote connection and shall be limited to system administration personnel only. All server administrator accounts shall comply with the password requirements set by password security policy.
8. 2 factor authentication mechanisms shall be required to administer servers.
9. Service accounts used to access system resources shall not be used for any other purpose. Only system administrators are permitted to have knowledge of service account credentials.
10. Servers will be located in access-controlled and environmentally protected facilities in accordance with physical and environmental security policy and procedures.
11. All servers shall run licensed version of operating system and applications.
12. Each server's configuration must be thoroughly documented, and this documentation must be kept up to date.

Virtualization Security

1. Virtual systems will be subjected to security controls to reduce any risk of attacks. The implemented configurations shall be reviewed on a frequent basis.
2. Access to the host system shall be provided only to the authorized administrators in the virtualized environment.
3. The operating systems shall be enabled with only necessary services and such services shall be documented.
4. BIOS password shall be used for both guest and host operating systems.
5. Host and Guest systems shall have clock synchronization.
6. Management of hypervisor shall be restricted to only the named administrators based on segregation of duties.
7. Creation of VM shall be restricted to the capacity of the host system. The creation of new guest systems shall be appropriately authorized through the change management process.
8. Logging and monitoring shall be carried out.
9. The network access to the Host system shall be restricted to management services only.
10. Appropriate firewall shall be placed to protect host OS and other guest OSs, where applicable.
11. Remote published infra VDI services need to have appropriate usage processes

Reference

SI No	Standard Name	Control Reference
1	ISO 27001:2013	A.15.2.1, A.15.2.2,