Policy Group	IT Services	**Policy Number**	SUP-ITS-03	جامعة زايد ZAYED UNIVERSITY
Responsible Office	Office of the CAFO	**Distribution**	External	
Date Approved	7 October 2020	**Effective Date**	7 October 2020	
Date Last Reviewed	5 November 2019	**Due Date for Next Review**	5 November 2022	

PROCEDURES
Access Control

Contents

A. Approved Authentication Services

1. In accordance with the Zayed University Access Control Policy, all Zayed University (ZU) equipment, networks and business systems must identify and authenticate ZU users by an Information Technology Department (ITD) approved authentication service.
2. ITD approved authentication services include Active Directory and Web SSO. Active Directory shall be the central authentication source for all types of logon accounts, applications and devices.

B. User Registration

1. The User ID Registration Procedure governs the authorization, deactivation and deletion of accounts.
2. HR Management System (HRMS) shall be the authoritative source for provisioning and de-provisioning of employee accounts into Active Directory, Applications and other services. General computing accounts and services are provisioned based upon employee affiliation and status on the HRMS, such as whether an employee is active or has resigned from the university.
3. The Banner System shall be the authoritative source for provisioning and de-provisioning of student accounts into Active Directory, Applications and other services. General computing accounts and services are provisioned or de-provisioned based upon student affiliation and status on the Banner, such as whether a student is active or has graduated from the university.
4. The HR Management System (HRMS) shall be the authoritative source for provisioning and de-provisioning of temporary/contracted employees/consultants into Active Directory, Applications and other services.

C. User Access Management

1. All users shall follow the Password Security policy (SUP-ITS-16).
2. All users of the ZU information system shall have a unique ID that can identify an individual user.
3. Roles and privileges shall be created with the minimum privileges needed for the user to carry out their role.
4. End users shall be presented with the Acceptable Usage policy (SUP-ITS-11) and be required to acknowledge and agree to the policy before being granted access.
5. End-user account creation, deletion and modification shall follow an account management process.
6. End-user accounts shall be disabled when the user leaves the university.
7. Requests for special accounts and privileges (such as vendor accounts, application and service accounts, system administration accounts, shared / generic accounts, test accounts and remote access) must be formally documented and approved by the requesting department manager.
8. Authorized user accounts (temp, third-party contractors/vendors, client representatives) shall be created/activated for a required period of time, as per the respective academic, administrative or business needs.
9. Application and service accounts must only be used by application components requiring authentication; access to the passwords must be restricted to authorized IT administrators or application developers only.
10. Employee access to ZU information systems and services will be granted based on the individual's job duties, project responsibilities and other business activities.
11. Department Heads will ensure that when an employee changes role within the university, their access will be amended so that it reflects the requirement of their new role. Any user access privileges to ZU business systems or services that are no longer required for the employee’s new role will be removed.
12. All user’s accounts that have been inactive for a period of three (3) months or more will be disabled and require the user's password to be reset through self-service or the ITD Service Desk before access is granted to Zayed University systems and services.
13. Suspension of user access for student accounts requires approval from the Student Affairs Deanship and the ITD Director and must be conducted in accordance with student misconduct regulations.

D. Review User Access Management

1. Zayed University management reserves the right to revoke the system privileges of any user at any time.
2. ZU ITD will annually conduct an audit review of existing user accounts and their access rights to detect dormant accounts and accounts with excessive privileges. Examples of accounts with excessive privileges include:
   - 2.1 An active account assigned to external contractors, vendors or employees that no longer work for the Institution.
   - 2.2 An active account with access rights for which the user’s role and responsibilities do not require access.
   - 2.3 System administrative rights or permissions (including permissions to change the security settings or performance settings of a system) granted to a user who is not an administrator.
   - 2.4 Unknown active accounts.

3. ITD will provide the dormant account and user excessive privilege access report to the concerned ZU department’s head for review and to ensure that current access privileges to information systems and services are relevant and appropriate for each individual user.

E. Administrative Access

1. All support, application and operating system IDs shall be unique and able to be mapped to an individual.
2. A list of privileged users shall be maintained.
3. All administrative connections shall be controlled by a security device, filtering by typically source, destination IP address and TCP/UDP port numbers.
4. Where possible all default accounts shall be either:
   4.1 Disabled;
   4.2 Renamed with a password change; or
   4.3 Renamed.
5. All end-user and administrative access shall be logically and physically separated.
6. Generic administrative accounts shall not be used.
7. Administrative roles shall have only the privileges that are needed for system administration (e.g. Local Administrator rights as opposed to Domain Administrator rights). Session timers shall be configured for administrative accounts and roles, to log the user out after a set period of inactivity.

F. Test Accounts

1. Test accounts can only be created if they are justified by the relevant business area or project team and approved by the application owner, through a formal request to the IT Manager.
2. Test accounts must have an expiry date (a maximum of six [6] months). Maintaining test accounts beyond this date must be re-evaluated every ninety (90) days and approved appropriately.
3. Test accounts will be disabled/deleted when they are no longer necessary.

G. Contractors and Vendors Access Management

1. Contractor/vendor representatives will be required to sign a Non-Disclosure Agreement (NDA) prior to obtaining approval to access Institution systems and applications.
2. Prior to granting access rights to a contractor/vendor, the ITD must verify all the requirements have been complied.
3. The name of the contractor/vendor representative must be communicated to the ITD at least two (2) business days before the person needs access.
4. The ITD will maintain a current list of external contractors or vendors having access to ZU systems.
5. The need to terminate the access privileges of the contractor/vendor must be communicated to the ITD at least one (1) business day before the contractor/vendor representative’s need for such access ends.

H. Remote Access to Vendor / Contractor/ Third-Party

1. Remote access to vendor/contractor (inbound and outbound) of the ZU network shall be reviewed and approved on a case-by-case basis.
2. Vendor/Contractor locations and offices shall be reviewed before permitting any connections into the ZU network.

3. Non-disclosure agreements (NDAs) shall be in place before access is enabled into the ZU network for any commercial purpose (e.g. for vendors).
4. Vendor/Contractor access shall be enabled via individual accounts specifically created for the entity.
5. Remote access connections into the ZU network shall be approved, controlled, authenticated and timed. Once the time frame has ended the connection shall be closed and the session terminated. The password shall be changed, and the accounts will be disabled and only be enabled when needed.
6. System and application logs shall be reviewed after any remote maintenance has taken place.
7. All critical/sensitive systems remote access to vendor/contractor shall be enforced through SSL VPN.
8. Physical separation will be maintained between the ZU network and any third-party network.
9. Access for contractors, consultants or vendor personnel to critical business information assets will be provided only based on a contractual agreement. This includes:
   - 9.1 The terms and conditions under which access is to be provided;
   - 9.2 The responsibilities of the contractors, consultants or vendor personnel;
   - 9.3 Agreement by the contractors, consultants or vendor personnel to abide by ZU Information Security policy and associated security policies.

I. Application Level Access

1. ZU shall provide access to applications based on job responsibilities and business justification.
2. ZU ITD will implement proper physical or logical isolation controls for highly critical information systems and application environments.
3. The above-mentioned policy should be implemented by the following steps:
   - 3.1 List all the applications used, and deployed in the ZU;
   - 3.2 Categorize the applications by business units or division;
   - 3.3 Classify the criticality of listed applications as per the ZU Information Classification Guidelines;
   - 3.4 Segregate the administrator-level access to database, storage and application.

J. Teleworking

1. ITD shall issue teleworking devices for the use of employee while teleworking. No privately-owned equipment (laptop/desktop) shall be used for teleworking.
2. While working from a home network environment, the teleworking employee shall ensure appropriate protections are in place on wireless networks.
3. The access rights set for a user working in the ZU IT environment remain in effect while teleworking from remote locations.
4. The physical security of the equipment used for teleworking shall be the responsibility of the employee member to whom it has been issued.
5. In case of theft/loss of the equipment, employee should immediately report/inform the IT Service Desk and a security incident shall be logged.
6. Teleworking equipment, being the property of ZU, is subject to audit or monitoring by ITD. The custodian shall present the equipment for such audit as and when demanded by ITD.

K. Revision History

Date	Revision
7 October 2020	Approved by the President as Acting Vice-President (PD#92 of 2020).
6 January 2020	Updated the policy number to SUP-ITS-03 from SUP-ITS-12.
5 November 2019	Reviewed by CAFO Management Council and endorsed for further approval. Revisions as per requirement from Telecommunications Regulatory Authority (TRA) Regulations for Information Technology Security in Federal Entities: • Added Approved Authentication Services • Added User Registration • Updated and Renamed End-User Access to User Access Management • Added Review User Access Management • Added Test Accounts • Renamed Third-Party/Remote Access to Remote Access to Vendor / Contractor / Third-Party
8 April 2018	Approved by Vice President (VP Decision #65 of 2018) New Procedures