Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Information Security Identification and Authentication**
Regulation and Procedure Number:	**URP: 04.735**
Policy Owner:	**Finance and Administration and Information Technology Solutions**

POLICY STATEMENT

This University Regulation and Procedure ("URP") establishes the information security identification and authentication regulations and procedures for managing risks from user access and authentication into information assets through the establishment of an effective identification and authentication program. The identification and authentication program helps Texas Woman's University ("TWU") implement security best practices regarding identification and authentication into Information Resources owned or operated by TWU.

The scope of these regulations and procedures is applicable to all Information Resources owned or operated by TWU. All Users are responsible for adhering to these regulations and procedures. If needed or appropriate, information regarding roles, responsibilities, management commitment, and coordination among organizational entities are embedded within these procedures. The Policy Owner, as defined in URP 01.320: University Policy Development and Implementation, is responsible for managing the development, documentation, and dissemination of this URP.

APPLICABILITY

This policy is applicable to TWU Students, Employees, University Affiliates, and Guests.

DEFINITIONS

1. "Accounts" means an established relationship between a user and a computer, network, or information service.

2. "Authenticator" means a coded signal transmitted within an information systems message as a proof of genuineness (i.e., passwords/passphrases).

3. "Confidential Data Classification" or "Confidential Data" means data that is private, confidential by law, or otherwise exempt from public disclosure (i.e.

exemptions under the Texas Public Information Act, Social Security Numbers, personally identifiable Medical and Medical Payment Information subject to the Health Insurance Portability and Accountability Act ("HIPAA") of 1996, 45 C.F.R. 160, Driver's License Numbers and other government-issued identification numbers, Education Records subject to the Family Educational Rights & Privacy Act ("FERPA") (20 U.S.C. § 1232g; 34 CFR Part 99), financial account numbers or credit or debit card number in combination with any required security code or access code permitting access to an individual's financial account, or other University Data about an individual likely to expose the individual to identity theft).

4. "Cryptographic Module Authentication" means any combination of hardware, firmware or software that implements cryptographic functions such as encryption, decryption, digital signatures, authentication techniques and random number generation.

5. "Employee" means any individual at TWU who is hired in a full-time, part-time, or temporary capacity in a faculty or staff position, or in a position where the individual is required to be a student as a condition of employment.

6. "Guests" means any individual not affiliated with TWU.

7. "Information Resources" means an element of infrastructure that enables the transaction of data, designed to provide content and information services to Users. Information Resources include information in electronic, digital, or audiovisual format and any hardware or software that store and use such information (i.e., electronic mail, local databases, externally accessed, CD-ROM, motion picture film, recorded magnetic media, photographs, digitized information, voice mail, faxes). This definition also includes computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, cloud services, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e., embedded technology), telecommunication resources, network environments, telephones, fax machines, printers, and service bureaus. Additionally, Information Resources includes the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

8. "Information System" means a discrete set of Information Resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of Information.

9. “National Institute of Standards and Technology (NIST)” means a non-regulatory agency of the United States Department of Commerce that works in cooperation with various industries to promote innovation and industrial competitiveness by advancing measurement science, standards, and technology.

10. "Privileged Account" means an Information System account with approved authorizations of a Privileged User.

11. "Privileged User" means a user who is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

12. “Student” means a person taking courses at TWU, a person who is not currently enrolled in courses but who has a continuing academic relationship with TWU, or a person who has been admitted or readmitted to TWU.

13. “University Affiliate” means any individual associated with TWU in a capacity other than as a Student or Employee who has access to TWU resources through a contractual arrangement or other association. This includes the following individuals:

    a. Contractors and Vendors: an individual, business, or governmental entity that has a fully executed contract to provide goods or services to TWU. This includes employees of contractors or vendors and independent contractors.

    b. Employee of a Governmental Agency: an individual employed by a federal or Texas state agency.

    c. Employee of a TWU-Affiliated Institution: an individual who works for organizations that are tightly aligned with the University.

    d. Pre-Employment Individual: an individual who will be hired by the University and the hiring department has sponsored their access to TWU resources.

    e. Other University Affiliate: any individual who does not fit into any other category and needs access to TWU resources.

14. “Users” means TWU employees, contractors, vendors, or other people using a TWU Information Resource.

REGULATION AND PROCEDURE

I. Security Standards

A. Identification and Authentication (Organizational Users)

1. ITS will assign each User a unique identifier (i.e., username). A User's username and password together make up the User's authentication credentials.

B. Identification and Authentication (Organizational Users) | Multifactor Authentication to Privileged Accounts

1. Multifactor authentication shall be implemented for access to Privileged Accounts. Regardless of the type of access (i.e., local, network, remote), Privileged Accounts are authenticated using multi-factor options appropriate for the level of risk.

C. Identification and Authentication (Organizational Users) | Multifactor Authentication to Non-Privileged Accounts

1. Multifactor authentication shall be implemented for access to non-privileged accounts. A non-privileged account is a User's unique identifier (i.e., username) created after a User has an official organizational status. Multifactor authentication is required for all authentications to resources which access Confidential Data.

D. Identifier Management

1. ITS will manage Information System identifiers for Users and devices by:

a. Assigning each User or device a unique identifier;

i. User unique identifiers are authorized for creation after a User has an official status;

ii. User unique identifiers will be assigned at time of account creation and follow the naming convention of legal first initial, last name (e.g. jdoe). Numbers may be added to the end to ensure uniqueness (e.g. jdoe10);

iii. Device identifiers are assigned during the asset management process in Facilities Management;

iv. Device identifiers will consist of the TWU inventory asset number assigned by TWU Facilities Management, followed by "twu" (e.g., 1234567twu);

v. Servers may be assigned a normalized name to aid in operational clarity.

b. Managing accounts to prevent the reuse of unique identifiers; and

c. Retiring User identifiers to reflect the User's official status (Ex. identifiers for terminated Employees expire at time of termination). Device identifiers remain active until surplused by Facilities Management.

E. Authenticator Management

1. The management of User Authenticators protects Information Resources from unauthorized access, ensuring the confidentiality and integrity of those resources. In managing authenticators, ITS will do the following:

a. Manage an automated user account creation program that verifies User information from official Human Resource or student system record before an account is created, and assigns initial information system authorizations;

b. Manage an automated process for disabling user accounts, as necessary;

c. Establish automated reminders to annually refresh passwords, and disabling accounts that fail to refresh passwords;

d. Manage an automated process that removes account access when membership changes;

e. Require replacement of forgotten or compromised passwords, rather than reissuing the same password;

f. Protect the security of passwords in storage and transit; and

g. Require Users to change default or assigned passwords.

2. User account passwords that are over 365 days old from the date of password creation must be reset by the User. Failing to reset a password will result in loss of access to Information Resources. Exceptions to password reset requirements may be made to select privileged or non-User accounts (e.g. "service accounts").

3. ITS shall change the password of certain accounts when personnel with knowledge of the applicable password are terminated or leave the university.

4. Users must not share their TWU account(s), passwords, Personal Identification Numbers ("PIN"), Security Tokens (i.e. Smartcard), or any other information device used for identification and authorization purposes (to include their TWU voicemail PIN).

F. Authenticator Management | Password Based Authentication

1. To manage password-based authentication, ITS shall do the following:

a. Maintain a list of commonly-used, expected, or compromised passwords, and update the list periodically and when organizational passwords are suspected to have been compromised directly or indirectly;

b. Verify that new and updated passwords are not found on the list of commonly-used, expected, or compromised passwords;

c. Transmit passwords only over cryptographically-protected channels;

d. Store passwords using an approved salted key derivation function, preferably using a keyed hash;

e. Require immediate selection of a new password upon account recovery;

f. Allow User selection of long passwords and passphrases;

g. Employ automated tools to assist the User in selecting strong password authenticators; and

h. Enforce the following password requirements for all User accounts:

i. Must include at least one number (Example: 1,2,3);

ii. Must include at least one uppercase letter (Example: A, B, C);

iii. Must include at least one lowercase letter (Example: a, b, c);

iv. Must include at least one of these symbols and no other symbols: ! @ # $ % & _ -

v. Must contain at least 10 characters;

vi. Must not be longer than 30 characters;

vii. May not repeat any character more than twice in a row;

viii. May not include User's username;

ix. May not include User's first name;

x. May not include User's last name; and

xi. Must not be reused or recycled.

2. All non-User accounts must follow, at minimum, the password requirements for User accounts. Non-User accounts passwords may have additional character length and complexity. Non-User account passwords may not be reused or recycled.

G. Authenticator Feedback

1. ITS will take the following measures to ensure that authentication information is protected:

a. Information Resources are configured to mask passwords by default;

b. Information Resources are configured to not indicate which part of the username/password combination is incorrect.

H. Cryptographic Module Authentication

1. ITS will take the following measures to ensure that Cryptographic Module Authentication meets the requirements of applicable federal laws, directives, policies, regulations, standards, and guidance:

a. Encrypt Data in transit and at rest where applicable;

b. Known vulnerable or weak encryption methods should be avoided;

c. The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Information

Resource Manager (“IRM”) or Information Security Officer (“ISO”); and

d. TWU’s encryption standards will be reviewed and upgraded as technology allows.

I. Identification and Authentication (Non-Organizational Users)

1. The ITS account management system uniquely identifies and authenticates University Affiliates using TWU systems and networks.

J. Re-Authentication

1. Users shall be required to re-authenticate after session timeouts, when roles, authenticators, credentials, security categories of Information Systems change, and when the execution of privileged functions occurs.

II. Regulatory Compliance

A. The State of Texas has chosen to adopt a select number of Identification and Authentication (“IA”) principles established in NIST SP 800-53 “Identification and Authentication” guidelines. The NIST IA controls have been assigned a number; however, the State of Texas has not adopted every NIST IA control, so there are gaps in the numbering sequence. The following subsections outline the IA standards included in TWU’s regulations and procedures.

1. IA-1, IA-2, IA-2(1), IA-2(2), IA-4, IA-5, IA-5(1), IA-6, IA-7, IA-8, and IA-11.

III. Compliance

Employees that violate this policy are subject to corrective and disciplinary action, including and up to dismissal, in accordance with TWU’s URP 02.330: Faculty Responsibilities, Standards of Conduct, and Disciplinary Processes and URP 05.600: Staff Standards of Conduct and Disciplinary Process. TWU may also take corrective action against interns, volunteers, contract employees, contractors, and/or consultants that violate this policy, including and up to termination of TWU’s relations or access with that individual or entity. Students that violate this policy are subject to corrective and disciplinary action, including and up to suspension or expulsion, in accordance with TWU’s URP 06.200: Student Code of Conduct.

REVIEW

This policy will remain in effect and published until it is reviewed, updated, or archived. This policy is to be reviewed once every six years. Interim review may be required as a

result of updates to federal and state law or regulations, Board of Regents policies, or internal processes or procedures.

REFERENCES

Tex. Admin. Code, Ch. 202

Department of Information Resources Security Standards Catalog

NIST Special Publication 800-53 (Rev. 5), Security and Privacy Controls for Information Systems and Organizations

URP 01.320: University Policy Development and Implementation

URP 02.330: Faculty Responsibilities, Standards of Conduct, and Disciplinary Processes

URP 05.600: Staff Standards of Conduct and Disciplinary Process

URP 06.200: Student Code of Conduct

FORMS AND TOOLS

None

Publication Date: 07/02/2021

Revised: 10/08/2021; 10/26/2021; 02/28/2024