UT - Martin Policy: IT1001-M - Account Procedures and Guidelines	
Version: 7	Effective Date: 06/09/2023

Objective:

This document describes the procedures for assigning accounts at UTM. It is intended to help users understand how and when accounts are created and deleted, and how notifications are made. It also emphasizes elements of the Acceptable Use Policy (AUP) regarding email.

Scope:

These guidelines apply to all users of, and information technology (IT) resources owned, operated, or provided by the University of Tennessee at Martin (UTM) including its regional centers.

"Users" includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the University's information technology resources.

Information transmitted or stored on University IT resources is the property of the University unless it is specifically identified as the property of other parties.

Principles:

The University has chosen to adopt the policy principles established in the National Institute of Standards and Technology (NIST) 800 series of publications.

UTM must develop or adopt and adhere to a program that demonstrates compliance with related policies and standards. These procedures and guidelines are the responsibility of the Position of Authority.

Each User of University resources is required to be familiar and comply with University policies. Acceptance is assumed if a user accesses, uses, or handles University resources.

Roles and Responsibilities:

Vice Chancellors, Deans, Department Heads: Sponsoring accounts affiliated with their responsible departments / areas.

Faculty/Staff Account Creation:

The Faculty/Staff account creation process begins when new hires are entered into the IRIS system with an "active" or "pending" status. This process must take place prior to an email account being assigned. On the third day after the new hire has been entered into IRIS, an automatic email will be sent to the department head requesting the following information:

- Is the new hire considered faculty?
- Is the new hire considered staff?

Once this information is received by Information Technology Services (ITS), the email account is created, and an automated email is sent to the department head containing the new hire's email address, password scheme, and other pertinent information. The new hire's email account will generally be available for use on the first business day following the reply by the department head with the requested information.

Security awareness training must be completed within 30 days for the account to remain active. The department head will be notified in the original email and the employee will receive an email with instructions for security awareness training. More information on security awareness training requirements can be found in *IT0123-M - Security Awareness, Training, and Education Program*.

New employees have 30 days to enroll in Two-Factor Authentication (2FA), after which the account will be automatically enrolled.

Student Account Creation:

Student accounts are created once they are admitted.

Faculty/Staff Account Deletion After Termination:

The Faculty/Staff account deletion process begins when current employees are terminated in IRIS. When the employee is terminated in IRIS, an automated helpdesk request is generated for the account to be deleted. The account is then set to expire 30 days after the employee's termination date. The account is then deleted 30 days after the expiration date. The former employee cannot access the account after the expiration date without assistance from ITS.

Student Account Deletion:

Students will have access to their Google account for one year after graduation.

Existing alumni who graduated before May 6, 2023, will have access to their accounts until January 31, 2024.

Retiree Account Deletion:

Retirees will retain access to their UT email account for 30 days from their last day of employment, after which the account is deleted according to the faculty/staff account deletion process.

Retirees who left the University before July 1, 2023, may keep their accounts if they maintain sponsorship from their department or organization.

Disabled Account Deletion:

Accounts that have been disabled for a year will be deleted.

Post-Retirement Accounts:

If a retiree returns to work at UT Martin post-retirement, they will use their existing account. If they do not have an account, one will be created according to the faculty/staff account creation procedures. Once the retiree's work assignment ends, deletion of the account will follow the retiree account deletion process, unless they already have a sponsored account.

Sponsored Accounts:

Anyone who is not a regular employee of the University and has an account must have their accounts sponsored. Department heads are responsible for the accounts sponsored by their department. Friends of the University (e.g., WUT, Sodexo, etc.) must be sponsored by the Vice Chancellor of Finance and Administration. The appropriate person will receive an email to approve the sponsored account. Sponsored accounts must be reviewed and renewed annually. The progress will be tracked in the current ITS ticketing platform.

Special Circumstances:

Accounts may be created, deleted, or continued by ITS as directed by the Chancellor's Office. Any special request should be routed through the respective division to the Chancellor's Office for approval.

Litigation Holds:

UT Legal Counsel may place litigation holds on existing email accounts resulting in those accounts remaining on the email system until Legal Counsel directs that it may be deleted.

Email Forwarding:

Automatic forwarding to external / personal email addresses from University email accounts is not allowed. Faculty and staff can request an exemption to forward to qualifying domains.

Exceptions:

Exceptions are handled on a case-by-case basis.

Acceptable Use:

The University of Tennessee at Martin has adopted the system-wide policy for the acceptable use of information technology resources.

All users have a responsibility to know and comply with University policies. Acceptance of University policy is assumed if a user accesses, uses, or handles University resources, which includes email. Examples of prohibited email use include, but are not limited to:

- Intentional eavesdropping or intercepting other users' emails
- Introducing, creating, or propagating spam or phishing emails
- Use for commercial purposes, except as specifically permitted under other written university policies or with the written approval of the Campus Authority
- Political campaigning or advertising on behalf of any party, committee, agency, or candidate for political office
- Engaging in activities that violate state or federal law, University contractual obligation, or another University policy or rule including but not limited to Human Resources policies and Standards of Conduct for students
- Misrepresenting one's identity to impersonate another user or send fraudulent emails
- Transmitting materials that, in doing so, is a violation of copyright law or infringement.

References:

IT0110 - Acceptable Use of Information Technology Resources

IT0110-M - Acceptable Use of Information Technology Resources

IT0123-M - Security Awareness, Training, and Education Program

Definitions:

Email (Electronic mail): A means or system for transmitting messages electronically.

IRIS (Integrated Resources Information System): The University branded enterprise resource planning system providing financial, human resources, payroll, procurement, and budgeting functionality across all campuses and institutes.

Phishing: Tricking a user into revealing personal or confidential information, such as a password.

Spam: Unsolicited bulk messages sent through email.

Two-Factor Authentication (2FA): A method of confirming a user's claimed identity by requiring a combination of two different components, which includes something you know (password, PIN), something you have (smart card, token), and something you are (biometrics).