Illinois Wesleyan University
Information Technology Services Email Use and Account Management Policy

Policy Synopsis

Title: Email Use and Account Management
Approval Date: XX/XX/XXXX
Revision Date, if applicable:
Review Date(s):
Responsible Officer (RO): Director of Security and Infrastructure
Standard Operating Procedures Manager (PM): Systems Administrator

A. Purpose and Scope

Purpose
This policy outlines the guidelines for email use and management at Illinois Wesleyan University (IWU). It is important for users to adhere to this policy to maintain the security, confidentiality, and integrity of IWU's email systems and data.

Scope
This policy applies to all IWU faculty, staff, students, affiliates, and contractors who have been granted access to IWU's email systems.

B. Email Accounts

IWU provides email accounts to faculty, staff, and students for the purpose of communication related to their academic and professional duties. All email accounts will be terminated at the end of employment. All student accounts will be terminated three years after graduation.

C. Email Use

IWU's email systems are for official university business and communications only. Personal use is not recommended as it may interfere with an individual's duties or violate any University policies. Users are prohibited from using email for any illegal or unethical purposes. Email

communication should be professional, respectful, and free from discriminatory or harassing language.

D. Email Management

Users are responsible for managing their own email accounts and ensuring that they comply with this policy. Users should regularly review and delete any unnecessary emails to conserve storage space and maintain an organized mailbox.

E. Security and Confidentiality

Users must take appropriate measures to ensure the security and confidentiality of their emails. Passwords must be kept confidential and not shared with anyone. Emails containing sensitive or confidential information must be encrypted or otherwise protected to prevent unauthorized access.

F. Access Management

Access to email accounts will be managed according to the following guidelines:

- **Faculty/Staff:**
  - Faculty and staff are granted access to an IWU email account upon hire.
  - Email accounts will be terminated at the end of employment
  - Faculty and staff are responsible for managing their own email accounts in accordance with this policy.
  - Inactive faculty and staff accounts will be disabled after 90 days of inactivity.
  - Email forwarding to external recipients is not recommended for faculty and staff.

- **Students:**
  - Students are granted access to an IWU email account upon enrollment.
  - Email accounts will be terminated three years after graduation.
  - Students are responsible for managing their own email accounts in accordance with this policy.
  - Inactive student accounts will be disabled after 180 days of inactivity.
  - Email forwarding to external recipients is not recommended for students.

- **Affiliates:**
  - Affiliates may be granted access to an IWU email account as needed for the performance of their duties.
  - Email accounts will be terminated at the end of their affiliation or agreement
  - Affiliates are responsible for managing their own email accounts in accordance with this policy.
  - Inactive affiliate accounts will be disabled after 30 days of inactivity.
  - Email forwarding to external recipients is not recommended for affiliates.

- **Employment and Alumni Status for Email Accounts**
    - If an individual is an employee and alumni of the University, upon leaving, they will be subject to the email account policy for employees. This means that their email account will be terminated at the end of their employment
- **Contractors:**
    - Contractors may be granted access to an IWU email account as needed for the performance of their duties.
    - Email accounts will be terminated at the end of their contract or agreement
    - Contractors are responsible for managing their own email accounts in accordance with this policy.
    - Inactive contractor accounts will be disabled after 30 days of inactivity.
    - Email forwarding to external recipients is not recommended for contractors.

G. Accessing Email Accounts

IWU reserves the right to access email accounts, despite the fact that a user has established login credentials. However, IWU and its agents or custodians of the email system will not access or disclose the content of an individual's email account unless there is a legitimate business need, or unless required by law.

In addition, before accessing or disclosing the content of an individual's email account, permission must be secured from an appropriate member of leadership designated for each constituency. The authorized leaders for each constituency are as follows:

Constituency	Authorized Leader
All Groups	University President
Advancement	VP of Advancement
Business and Finance	VP of Business/Finance
Enrollment and Marketing	VP of Enrollment/Marketing
External Relationships	VP of External Relationships
Institutional Effectiveness	Assoc. VP of Institutional Effectiveness
Provost/Dean of Faculty	Provost/Dean of Faculty
Student Affairs/Dean of Students	VP of Student Affairs/Dean of Students

*In situations where the authorizers listed above are unable to perform this duty in the manner or period needed, a designee of the University President will assume decision authority.

Furthermore, IWU reserves the right to monitor and review email accounts for compliance with this policy and applicable laws and regulations.

H. Data Backup and Retrieval upon Employee Departure

When an employee leaves the University, each department has the right to request a backup of all files and emails to a shared departmental drive by submitting a helpdesk request at it@iwu.edu.

Additionally, staff and faculty may request a backup of their personal data to a personal device prior to departure from the University by submitting a helpdesk request at it@iwu.edu.

I. Exceptions

All exceptions to this policy must be approved by the University President or designee.

J. Legal and Regulatory Requirements

IWU complies with the Illinois Information Security Act (IL 815) and the Gramm-Leach-Bliley Act (GLBA) requirements to protect the confidentiality, integrity, and availability of University data.

K. Violations

Violations of this policy may result in disciplinary action, up to and including termination of employment.

L. Related Information

Not applicable.