	Last Approved	N/A		Area	Information Technology/ Management (Procedures)
UNIVERSITY OF WEST GEORGIA	Effective	N/A			
	Next Review	N/A		Chief Or Responsible Office	Chief Information Officer

User Account Management

Authority for Procedure granted by UWG Policy 5002, Data Security.

A. Purpose

This procedure establishes guidelines for the appropriate use and administration of Information Technology (IT) at the University of West Georgia (UWG). It works with associated procedure UWG PL 5001, Acceptable Use for Computers and Network, and defines Users' expected behavior and responsibilities. Users are required to accept these IT procedures as a condition of their access to the University's IT Facilities. This procedure focuses explicitly on administering User Accounts for authorized Users of the University's IT Facilities.

B. Application & Scope

This procedure applies to all IT accounts at UWG, and it is essential that Users understand their responsibilities and legal obligations outlined within. In a conflict between a University Policy or Procedure and a divisional/unit-level guideline, the University's Policy or Procedure will control.

C. Account Holder Entitlements

Account holders at UWG are granted access to a wide range of computing and networking facilities, including email, internet access, calendars, and systems integrated with the University's account management system. The level of access granted is determined by the privileges associated with the account type and any specific system access assigned to the account holder. Requests for exceptions to the standard account privileges may be considered upon written request and approval by the appropriate divisional Vice President.

D. Account Privacy Concern

Accounts and data on any UWG email service may be subject to legal discovery or a public records request made to the University. This means that UWG may be legally obligated to release your information to the requestor, even if it is of a personal nature. This exposure applies to any email sent and received on a UWG email service. Moving personal emails to a private email service will prevent your data from being exposed in this way. (see Georgia Open Records Act O.C.G.A.§§ 50-18-70 — 50-18-78)

E. Account Types

Below are the account types issued and managed at UWG.

1. Employee Accounts

Employee accounts are provided to compensated employees (faculty or staff) of UWG and individuals with honorary academic appointments, such as honorary or visiting fellows, if they meet the employee creation requirements (otherwise classified as a vendor). These accounts are intended for work purposes only and are issued for the duration of employment and deactivated at the end of employment.

i. Administration and Implementation

The onboarding processes, including new employee email creation and access to UWG systems, are handled by the UWG hiring managers responsible for coordinating employee recruiting efforts with their respective Office of Human Resources (OHR) representative.

To create an employee account, the OHR or the hiring authority must submit a request to the Information Technology Services (ITS) Service Desk at servicedesk@westga.edu and include the following required information:

- Name (first and last as it appears in Banner)
- 917 Identification Number
- UDCID - a globally unique identification number that is assigned to each Banner User
- Employee ID number - this information is optional at creation but required before accessing some systems.
- Unit name
- Immediate supervisor, if possible

Once the OHR or the hiring authority receives confirmation from ITS, account information is added to the hiring package for employee acknowledgment. By accepting employment with UWG, the individual acknowledges their acceptance of UWG policies and associated procedures.

Each employee account is assigned a unique username based on the account holder's name, typically using the first character of the first name followed by the last name (e.g., jdoe@westga.edu). In cases of duplicate names, variations are used to ensure uniqueness.

ii. Student Employment Accounts

Student employment accounts are specific to students who hold positions (i.e., SA, TA, GA, GRA, FWSP, etc.) within a unit. The hiring manager or supervisor submits the request to servicedesk@westga.edu requesting the new student employment account. (see section E1 for required data elements). These accounts follow a naming convention that includes the unit abbreviation and the student account (example: its-jdoe1). Student Employment accounts expire at the end of each semester and must be renewed by the manager or supervisor.

iii. Alias

Aliases may be created in specific scenarios, such as ensuring email delivery due to account changes, using a User's full name in an email address, or truncating email addresses with character limits. (See attachment Differences between Alias and Generic Accounts)

Aliases should follow the same naming conventions as employee accounts when possible. An alias may route email to another class of account to reduce the number of accounts, such as generic@westga.edu sending to the jdoe@westga.edu account.

iv. Account Closure & Deletion

Employee accounts remain Active if the account holder has a current or future appointment with the University. An appointment is considered concluded on the last date of paid employment or affiliation with the University. To facilitate the proper closure of an employee account, the immediate supervisor must complete the Termination and Transfer Notification Form for faculty, staff, or student employees.

For employees transferring between units within UWG, immediate supervisors must complete the Termination and Transfer Notification Form for access management.

ITS may reactivate Closed User Accounts for data retrieval purposes. Access may be granted to the employee's supervisor or the supervisor's designee upon submission of a request to the ITS Service Desk at servicedesk@westga.edu. However, access to the account will be limited based on specific data retrieval requirements and a time restriction renewed in 90-day increments. If the account still exists, individuals resuming employment with UWG may have the account reinstated with the original username. Account usernames should not be reissued to other users.

2. Student Accounts

i. Creating a Student Account

A Student account is established when an individual attains acceptance or active status in the Student Information System. Each student account is assigned a unique username based on the name followed by a numerical value, such as jdoe1 for John Doe. Student email addresses end in @my.westga.edu A student can only possess one student account at any given time.

Prospective students may be issued a pre-admit account granting access to minimal systems to facilitate the application process.

ii. Closing and Deleting a Student Account

Continued access to a student account is based on the student's enrollment or Active status in the University Student Information System. A student account will be marked Closed six months after course completion or graduation. This process is governed by the Registrar's Office and controlled within the University Student Information System.

Students receive email notifications to their affected account when it is identified for automatic closure. Reactivation occurs under the original username if the account still exists.

Closed student accounts enter a cycle where access is limited to necessary resources for reapplication or transcript recovery. Data from Closed student accounts beyond that requirement is purged in batches after all of the following criteria are met:

- 18 months from the last enrolled semester
- no future enrollment is on record.

Deleted student account usernames are not reissued. Student Accounts are only deleted in case of duplication or technical issues.

3. Generic Email Accounts

Generic accounts are intended for work purposes only and are issued for the duration and deactivated upon the end of their functional purpose. By default, generic email accounts are restricted from accessing other applications or systems. If additional access is required, such requests will be reviewed based on necessity without compromising a secure generic email account, which refers to an email account that is not tied to any specific individual or UWG unit. Its purpose is to provide a centralized point of contact for multiple individuals or units and to meet general needs like support, contacts, or communication within the University. Rather than being named after a specific person, generic accounts are usually named according to their purpose or function (e.g., servicedesk@westga.edu). (See attachment Differences between Alias and Generic Accounts)

Note: Generic email accounts have one designated owner who knows the account's password. However, other Users can access the account through the delegation feature.

Only faculty or staff are eligible to request the creation of a generic account, and any data sharing or changes related to the account must be under the account owner's authorization.

Only the designated owner of a generic email account may request changes to the account. In cases where the owner is no longer affiliated with the unit or University, the current owner or unit head should contact the ITS Service Desk at servicedesk@westga.edu to designate a new owner.

Generic email accounts will remain open unless closure is requested by the account owner, unit head, or the account is abandoned. When an account is Closed, the same deletion rules applicable to employee accounts will be followed, with the termination date of the generic email account set as the closure date.

To request the creation or closure of a generic email account, email the ITS Service Desk at servicedesk@westga.edu.

4. Vendor Accounts

Vendor accounts may be created for individuals requiring access to University ITS Facilities through their affiliation with UWG or one of its subsidiaries. Exceptions may be granted at the discretion of ITS, such as when a visiting academic is involved in teaching and needs to appear as a UWG employee. The following affiliations are recognized.

    i. Service providers (e.g., third parties, contractors, consultants, agents, etc.) of the University or its subsidiaries typically involves a contractual agreement (see UWG PL #1008, Contract Management and associated procedure)

    ii. Affiliated businesses and organizations of UWG. (See procedure Affiliated Organizations)

Vendor accounts are only issued an email address when a technical need is established. Vendor accounts are assigned a unique username abbreviation, "ven-." A vendor User Account's email address is ven-username@westga.edu (e.g., ven-jdoe@westga.edu).

Aliases may be created in specific scenarios, such as ensuring email delivery due to account changes. If an alias is required, it should follow the same format as employee email aliases when possible.

To request vendor account creation, the Vendor must complete the Outside Entity Network/Remote Access Request Form. *(see attachment)*

All Vendor accounts require an expiration date that shall not exceed 12 months. Access may be renewed by re-submitting the Outside Entity Network/Remote Access Request Form.

5. Emeriti /Retiree Accounts

    i. **Retirees (non-Emeriti)** faculty or staff are not eligible for a UWG account. Faculty and Staff who plan to retire need to begin migrating any personal emails to a personal email account prior to their last day.

    ii. **Emeriti accounts** are exclusively created through the migration process from employee status and shall not be recreated after deletion. These accounts are issued to former faculty or administrative staff holding emeritus status. These accounts are intended for UWG-affiliated research and educational purposes only and are given for the duration of emeriti status unless revoked, Withdrawn, or declined upon offer.

        An emeriti will have their email address adjusted to end with @emeriti.westga.edu. (e.g., jdoe@emeriti.westga.edu). Emeriti will retain access to data (e.g., employee account emails, settings, etc.)

6. Affiliated Non-Employee

Affiliated Non-Employee email accounts support official university business and communication needs of the University President. Only the President's spouse or partner is eligible when their role directly advances the university's mission, such as coordinating events, engaging in alumni or philanthropic

efforts, or serving in a public-facing capacity, and requires email access.

These accounts are restricted from accessing other university applications and systems and are not eligible for an alias. Affiliated Non-Employee email accounts remain active until the sponsoring executive (i.e., University President or their designee) requests closure or is deemed abandoned. The sponsor executive is responsible for ensuring appropriate use and notifying ITS when access is no longer needed. Upon closure, standard employee account deletion rules apply.

To request an account, the sponsoring university executive or designee must submit a written request to the ITS Service Desk at servicedesk@westga.edu with justification, business purpose, and expected duration. All requests are subject to case-by-case review and require approval by the Chief Information Officer (CIO) or designee.

7. Public Accounts

Public accounts are intended for public use to access limited services and information and are deployed in environments where computer sharing is essential, such as labs or kiosk-type stations. The allowances and restrictions of public accounts are tailored to their specific purpose. Permissions are carefully reviewed to mitigate potential risks and prevent access to most systems. When feasible, the default choice for a particular need will be to use an account assigned to an individual, such as an employee or student account, at the discretion of ITS.

8. Service Accounts

Service accounts are exclusively established for applications or automated processes only and deactivated upon the end of a functional need or contract. These accounts are granted only the necessary permissions to perform their designated functions. The management of service accounts is typically handled by ITS personnel and generally restricted from access by individuals outside ITS.

F. Account Review

Account reviews are conducted annually to ensure the validity and appropriateness of accounts. Additionally, ITS retains the right to audit accounts to verify their Active Account Status and revise the account issuance, closure, and/or deletion criteria.

G. Account Closure & Deletion

Account closure involves freezing the account, revoking the password, and potentially deleting data after 18 months of inactivity centered around the end of the semester unless under a legal hold. Except for Student Accounts, accounts are deleted by returning them to the separated account pool with an effective termination date of the closure date.

H. Account Access Withdrawal

ITS has the authority to Withdraw access to an account with prior notification to the Chief Information Officer. In cases of suspected policy or procedure violations or account compromises, account access

may be temporarily Withdrawn. Furthermore, accounts may be Withdrawn due to abandonment if they show no activity for twelve months. ITS will close the account once satisfied that the account is abandoned. An email notification will be sent to OHR, hrservices@westga.edu when an emeriti or employee account is determined to be abandoned.

I. Compliance

Before account activation, users must:

- Acknowledge and agree to comply with UWG policies and procedures, including but not limited to Acceptable Use for Computers and Network, Data Security policies and related procedures.

- Complete all required compliance training, including Cybersecurity Awareness Training.

- Use the account for university-related communications and activities.

- Acknowledge that account activity is subject to monitoring and auditing in accordance with university policies.

- Acknowledge that email communications are subject to the Georgia Open Records Act (O.C.G.A. § 50-18-70 et seq.) and may be disclosed in response to public records requests.

Failure to meet these requirements may result in account suspension or deactivation.

Users are encouraged to report any security misuse to the Cybersecurity Officer or the ITS Service Desk at servicedesk@westga.edu, and such reports will be treated with sensitivity. For issues that go beyond security, see the Complaint and Appeals webpage.

Definitions

Account Status - user accounts can have different statuses, including active, expired, closed (deactivated), and withdrawn (restricted), each with specific implications and conditions.

- **Active** - an active account is a fully operational account,

- **Expired** - an expired account is one where the account expiration field has expired and is required to be renewed before the account can be used,

- **Closed (deactivated)** - a closed (deactivated) account is one where access to the account is revoked given that the Account Holder no longer satisfies the criteria for holding that type of UWG account (Note the University retains closed accounts for a defined period after which time they are deleted. Until deleted, the account can be reinstated to the Account Holder),

- **Withdrawn (restricted)** - a withdrawn (restricted) account is one where the User's access to the account is removed completely or in part before the official closure of the account. This is a temporary status and transitions to active or closed once an issue is resolved.

IT Facilities - facilities operated by the University, whether owned or leased.

User - anyone using the University of West Georgia's Information Technology Facilities or accounts.

User Account - an authorized user account provided to a user to be used solely by that user for the purpose of accessing services as granted to that user account.

Resources

- UWG PL 5001 Associated Procedure: Acceptable Use for Computers and Networks
- UWG PL 1009 Legal and Regulatory Compliance and associated procedure Legal Holds and Records Preservation

Keyword

list-serv

Attachments

🖇 Generic email v. Google Groups_202308.pdf

🖇 Outside Entity Network_Remote Access Request Form (fillable).pdf

Approval Signatures

Step Description	Approver	Date