

Waycross College

IT System Accounts Policy

Effective Date: March 31, 2007
Last Revised: October 19, 2006

Status:

- Draft
 Approved

Responsible University Officer

Director of Computer Services

Responsible Coordinating Office

Computer Services

Online Publication

<http://www.waycross.edu/compserv/itpolicy/>

1. Scope

This College-wide policy addresses the creation, modification, and termination of information technology system accounts for all Waycross College employees. All accounts for Waycross College information technology resources are maintained by the Computer Services Department.

2. Policy

2.1. System Accounts for Employees

2.1.1. Account Creation Request for New Employees

All account creation requests must be submitted to Computer Services for approval and creation. In the case of new employees, the immediate supervisor, human resources and data owner fill out a Computing Accounts Creation Request form and submit it to Computer Services. Computer Services will review the form, consult with the employee's supervisor and other administrators on account access if necessary, and complete the creation of the accounts. Requests for access to systems or account permissions for which the employee has no job function responsibility will be denied. In an effort to ensure and enhance security, employees will be granted the minimum access rights to effectively perform their job functions.

2.1.2. Account Creation / Modification Request for Current Employees

All account creation / modification requests must be submitted to Computer Services for approval and creation. In the case of current employees, the employee or immediate supervisor

must submit the request in writing to Computer Services. Computer Services will review the request, consult with the employee's supervisor, data owners and other administrators on account access if necessary, and complete the creation of the accounts. Requests for access to systems or account permissions for which the employee has no job function responsibility will be denied. In an effort to ensure and enhance security, employees will be granted the minimum access rights to effectively perform their job functions.

2.1.3. Change in Access Needs / Job Functions

The immediate supervisor, employee, data owner, or human resources must promptly notify Computer Services in writing of any changes in employee job functions that would require a reduction in authorized access.

2.1.4. Account Termination Request for Departing Employees

In the case of a departing employee, the immediate supervisor or human resources must promptly fill out and submit a Computing Accounts Termination Notice to Computer Services. Computer Services will process the notice on the effective termination date or immediately upon receipt if the notice is received by Computer Services on or after the termination date, or if the employee separation is less than amicable. If the employee separation is less than amicable, the immediate supervisor or human resources should contact Computer Services via phone or email and request immediate action on the Computing Accounts Termination Notice.

2.1.5. Responsibility of the User

Users must not attempt to access systems or accounts for which they have no job function responsibility. The ability to access a system or account does not constitute authorization of such access. Authorization exists only for those users who have been granted access and have a job function responsibility to perform. Unauthorized access may result in disciplinary actions up to and including termination. If the unauthorized access constitutes a serious legal offence, legal affairs and law enforcement may be contacted as necessary. Users must not share their password or access to their account. Users are responsible for all activity performed with their user names.

2.1.6. Review of User Accounts

There will be a periodic review, at least once a year, by Data Owners and Computer Services of user accounts to determine whether permissions are still needed for the job responsibilities assigned. A periodic review may also be initiated anytime a job description changes or personnel changes occur. A Supervisor or Data Owner may also ask to review user accounts at any time, but the Data Owner is the only one that can authorize any changes.

2.2. System Accounts for Students

2.2.1. Account Creation Request for Students

Accounts for the student information access system (Banner Web) and online course management system (WebCT) are created automatically for students at Waycross College. Instructions for accessing the student information access system are provided to students by their advisors and / or the Student Services Department. Instructions for accessing the online course management system are provided to students by the instructor of their respective course. Students have the option of requesting a Waycross College student email account. Requests for

student email accounts are submitted via an online form on the Computer Services website. Once a request for student email has been submitted, Computer Services verifies that the student is currently enrolled, creates the email account, and provides access information and instructions to the student.

2.2.2. Account Modification Request for Students

Modification to student information access system and online course management system accounts are handled by addressing the cause for need of the modification. For example, if a student needs his or her name changed in the online course management system, they are informed the name is pulled directly from the student information access system and that they will need to submit the name change to the Student Services Department to have the student information access system updated. The name will then be automatically changed on the next update / upload of student information. Modification of student email accounts is handled by the Computer Services Department. Students need to contact Computer Services and explain the needed change. Computer Services will then verify any relevant information, such as the student name in the student information access system, and make the necessary account modifications.

2.2.3. Change in Student Status

Student account access is determined by the enrollment status of the student. Non-active students retain access to the student information access system; however their permission levels change automatically as different conditions are met. For example, a student who has taken two semesters off from school may log on to the system and register for classes for the next term. However, a student who has not taken classes in two years would have to reapply and be accepted before being able to register online. Online course management system access is automatically governed by the students' enrollment. Non-active students do not have access to the online course management system. Student email accounts are managed by Computer Services staff. At the beginning of each semester, after the add / drop period has ended, email accounts for students who are not actively enrolled in any classes are deleted from the system.

2.2.4. Responsibility of the User

Users must not attempt to access systems or accounts for which they do not have authorization. Unauthorized access may result in disciplinary actions, up to and including the maximum punishment prescribed in the student conduct code. If the unauthorized access constitutes a serious legal offence, legal affairs and law enforcement may be contacted as necessary. Users must not share their password or access to their account. Users are responsible for all activity performed with their user names.

2.3. Passwords

2.3.1. Password Creation

Waycross College promotes strong password construction as a first line of defense against improper access. Initial passwords are created for and provided to users by Computer Services. Users are instructed to change their passwords on systems which allow the user to change their own passwords. Not all characteristics of strong password construction are available on all systems. In such cases, users are instructed to follow as many construction parameters as possible. Strong passwords typically exhibit the following characteristics:

- At least 8 alphanumeric characters (Banner Web allows only 6)

- Upper and lower case characters
- Digits and special characters as well as letters, such as numbers (0-9) and other characters (!@#\$%)
- No identifiable words in any language, slang, dialect, or jargon
- No personal information, such as family names
- No null passwords or passwords which are the same as the user ID

2.3.2. Password Changes

Passwords on critical systems are to be changed at least every 90 days. Passwords on less critical systems are to be changed at least every 6 months. Users should not reuse passwords they have previously used and changed from.

2.3.3. Password Concerns

Any user who feels his or her password(s) may have been discovered by another person, should immediately change their password and inform Computer Services of the possible discovery. Computer Services may investigate any possible password discovery. Individuals found to have violated college policy by divulging their passwords or obtaining another person's passwords may be subject to disciplinary actions or legal actions.