Georgia College & State University

Milledgeville, GA

IT Access Controls Procedures

IT Access Controls

Table of Contents

Table of Revisions

Original Date: April 22, 2013

Revision Number:	Description:	Date:	Revised By:
1	Addition: Revize	May 7, 2013	D. Ivey/M. Voight
2	Modify PAWS Access	July 31, 2013	H. Patrick

Introduction

Georgia College and the University System of Georgia (USG) strive to minimize security vulnerabilities. To avoid vulnerability, Georgia College has established guidelines that detail the responsibilities of system owners, administrators, approvers, and users regarding the management of computer and network security. Thus, the information in this document outlines acceptable account management procedures. The procedures are in accordance to requirements set forth by the USG and Georgia College.

Georgia College and USG allow access authorization that gives the "user" the right to certain privileges within information systems. Access granted to the user does not imply any job or information privileges beyond those stipulated in the employment agreement or by Georgia College policies and/or procedures. The policies and procedures are effective regardless of the information's format e.g. automated, paper, or electronic. **In all circumstances, users shall follow Georgia College policy and/or state and federal regulations regarding access and rights to the institution's confidential and sensitive information.**

Purpose

Information systems must be protected from loss, contamination, destruction, and unauthorized access. Proper management and protection of information systems ensure that information entrusted to Georgia College attains a degree of protection commensurate with its value.

The following procedures address IT access controls. The procedures are valid for all Georgia College administrators, executives, faculty, staff, researchers, clinical care providers, and students.

Terms and Definitions

Confidential Information is information that if used or disclosed improperly could adversely affect the ability of the institution to accomplish its mission. Examples of confidential information are records about individuals protected under the Family Educational Rights and Privacy Act of 1974 (FERPA) and other applicable laws, or data not releasable under the Georgia Open Records Act or the Georgia Open Meetings Act.

A **Critical System** is a system whose failure or malfunction will result in not achieving organization goals and objectives.

The **Account Administrator** manages user's access to system information.

The **Principle of Least Privilege (PoLP)** describes minimal user profile or access privileges to information resources based on allowing access to only what is necessary for the users to successfully perform their job requirements.

Sensitive Information is information maintained by USG institutions, the USO, and the GPLS that require special precautions as determined by institution standards and risk management decisions to ensure its accuracy and integrity. Accuracy and integrity is ensured by using integrity, verification, and access controls to protect sensitive information from unauthorized modification or deletions.

A **System Owner** is the manager or agent responsible for the function that is supported by the resource or the individual responsible for carrying out the program that uses the resources. The system owner is responsible for establishing the controls that provide the security. The system owner of a collection of information is the person responsible for the business results of that system or the business use of the information.

Users are individuals who use the information processed by an information system.

Deactivation locks or denies the user's log on attempts.

The **Activity Journal** contains the operation(s) performed by the IT account administrator regarding information access.

A **Section** is an area of the website that is categorized in its own group, e.g. College of Business, Registrar Office, Student Government Association (department is too specific).

The **Section Supervisor** is manager of the user that has access to their respective section of the web.

Requirements

R1. Identify and classify information systems that process or store confidential or sensitive information, or are critical systems and document their owners and/or responsible party(s). A list of systems and owners will be created and produced upon request. (USG 3.1.1.3:1,2)

R2. Ensure appropriate resources are available and maintained to adequately authenticate and verify authorized access. Resources to prevent and detect unauthorized use shall also be maintained. (USG 3.1.1.3:5b-c)

R3. Follow appropriate procedures to ensure only authorized users are allowed physical, electronic, or other access. **Note:** The system owners, system access administrators, and users are all responsible for preventing unauthorized use. (USG 3.1.1.3:4,6)

R4. Document the procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

R5. Update system access no more than **5** business days after terminations and no more than **30** days after other personnel status changes. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:7,10)

R6. Revise and/or review user authorization upon notification of personnel status changes. The suggested parties responsible for notifications are system owners, managers, and human resources. (USG 3.1.1.3:8)

R7. Maintain an up-to-date mapping of users to information systems. Review user access information with system owners every **4** months. (USG 3.1.1.3:3,9)

Maintaining Systems Inventory

Requirements

R1. Identify and classify information systems that process or store confidential or sensitive information, or are critical systems and document their owners and/or responsible party(s). A list of systems and owners will be created and produced upon request. (USG 3.1.1.3:1,2)

Procedure

Georgia College has and regularly maintains an inventory list of critical systems. The list contains the following: system name, data/system owner, operational criticality, data sensitivity level, and other system identity specific information. This list is readily available upon request to the ISO.

Section 1: Banner

1.1 Authenticating Access & Preventing Unauthorized Use

Requirements

R2. Ensure appropriate resources are available and maintained to adequately authenticate and verify authorized access. Resources appropriate for preventing and detecting unauthorized use shall be maintained. (USG 3.1.1.3:5b-c)

R3. Follow appropriate procedures to ensure only authorized users are allowed physical, electronic, or other access. **Note:** The system owners, IT account administrators, and users are all responsible for preventing unauthorized use. (USG 3.1.1.3:4,6)

Procedures

1. System owners inform the prospective user about the importance of keeping their access information safe.

2. Users are prompted to create a specific password, and to create a new password every 3 months.

3. Accounts are locked after multiple failed attempts.

4. IT account administrators communicate with system owners to identify approved users and to grant, review, deactivate, update, and/or terminate account access based upon that communication.

5. To prevent and detect unauthorized access, IT account administrators monitor audits generated by the Banner system. Locked accounts are reviewed and unusual activity is investigated.

1.2 Granting Banner Access

Requirements

R4. Document the procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

Procedures

1. The system owner contacts the IT account administrator via email with an account creation request. Requests by phone and requests from non-system owners are not acceptable.

2. The IT account administrator creates account access after receiving proper notification and approval from the registrar.

3. The system owner receives account information from the IT account administrator when the account has been created. **Note:** Setting permissions on the account with regard to the principle of least privilege is the system owner's responsibility.

4. The system owner contacts the prospective user and instructs the user to contact the IT account administrator for a temporary password and other access information.

5. The IT account administrator documents the transaction in an activity journal.

1.3 Deactivating User Access & Updating Personnel Changes

Requirements

R4. Document the procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

R5. Update information system access no more than 5 business days after terminations and no more than 30 days after other personnel status changes. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:7,10)

R6. Revise and/or review user authorization upon notification of personnel status changes. The suggested parties responsible for notifications are system owners, managers, and human resources. (USG 3.1.1.3:8)

Procedures

1. To initiate and complete deactivation, the IT account administrator receives notification through EREQ, a weekly termination report, or information obtained from a system owner.

2. Within **5** business days of notification the IT account administrator:
   - Deactivates the user’s account
   - Removes all user privileges
   - Records such actions in the activity journal

Personnel Status Changes

1. Within **5** business days of a personnel status change notification, the IT account administrator deactivates the former account.

2. Updated access is granted when the system owner sends an official request.

1.4 Information System Access Review

Requirements

R4. Document the procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

R7. System owners will maintain an up-to-date mapping of users to information systems. IT account administrators will review user access information with system owners every **4** months. (USG 3.1.1.3:3,9)

Procedures

1. The IT account administrator provides the system owner with a list of users that have access to their system every **4** months. However, an up-to-date list of user accounts is available upon request to the CIO.

2. The IT account administrator modifies user access at the system owner's request.

3. The system owner acknowledges the list has been reviewed and responds via email.

4. The IT account administrator documents the transaction in the activity journal.

Section 2: PAWS (Banner Self-Service)

2.1 Authenticating Access & Preventing Unauthorized Use

Requirements

R2. Ensure appropriate resources are available and maintained to adequately authenticate and verify authorized access. Resources appropriate for preventing and detecting unauthorized use shall be maintained. (USG 3.1.1.3:5b-c)

R3. Follow appropriate procedures to ensure only authorized users are allowed physical, electronic, or other access. **Note:** The system owners, IT account administrators, and users are all responsible for preventing unauthorized use. (USG 3.1.1.3:4,6)

Procedures

1. The IT account administrator maintains tools that have been implemented to ensure users can readily acquire and change access information. IT account administrators **do not** assign account privileges and/or rights to the PAWS system.

2. The IT account administrator manages features within PAWS that control the information required to authenticate users.

3. The IT account administrator ensures that PAWS is shut down daily for back-up and/or installation appropriate patches.

2.2 Granting PAWS Access

Requirements

R4. Document the procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

Procedures

Students

1. The admissions personnel input user enrollment data into the system.

2. The system uses that data to generate an ID and password.

3. The student receives an enrollment packet with instructions on how to initiate access.

Faculty & Staff

1. Human Resources or Academic Services personnel input user employment data into the system.

2. The system uses that data to generate an ID and password. **Note:** The user's account access is at the lowest level of the principle of least privilege. Permissions are based on values in the EMPLOYEE table (Oracle/Banner instance) which is maintained by both Human Resources and Academic Services personnel.

2.3 Deactivating User Access & Updating Personnel Changes

Requirements

R4. Document the procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

R5. Update information system access no more than **5** business days after terminations and no more than **30** days after other personnel status changes. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:7,10)

R6. Review and/or revise user authorization upon notification of personnel status changes. The suggested parties responsible for notifications are system owners, managers, and human resources. (USG 3.1.1.3:8)

Procedures

Students

1. Student accounts are **never** deactivated or terminated. The accounts are consistently available to students as it has information concerning only that student.

Faculty

2. Faculty accounts are never deactivated or terminated. The accounts are consistently available to faculty members as it has information concerning the classes they administered.

Personnel Status Changes

1. Updates concerning terminations and personnel status changes are not applicable to student or faculty users.

2.4 Information System Access Review

Requirements

R4. Document the procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

R7. System owners will maintain an up-to-date mapping of users to information systems. IT account administrators will review user access information with system owners every 4 months. (USG 3.1.1.3:3,9)

Procedures

Students

1. Student accounts do not require review because their access is neither terminated nor updated.

Faculty & Staff

1. The system owner sends review request to the registrar account administrator.

2. The registrar account administrator adds permissions and/or removes access.

Section 3: Oracle Administrative Accounts

3.1 Authenticating Access & Preventing Unauthorized Use

Requirements

R2. Ensure appropriate resources are available and maintained to adequately authenticate and verify authorized access. Resources appropriate for preventing and detecting unauthorized use shall be maintained. (USG 3.1.1.3:5b-c)

R3. Follow appropriate procedures to ensure only authorized users are allowed physical, electronic, or other access. **Note:** The system owners, IT account administrators, and users are all responsible for preventing unauthorized use. (USG 3.1.1.3:4,6)

Procedures

1. A human resources administrator or IT account administrator informs the prospective user that the privileges allocated to them should only be used within the context of the job function and according to Georgia College policy and/or state and federal regulations.

2. The Enterprise Application Support team uses internal communication to identify approved users and to grant, review, deactivate, update, and/or terminate account access based upon that communication.

3. IT account administrators use specific ID and password combinations to prevent unauthorized use.

4. IT account administrators monitor system generated audits that reflect access attempts to detect unauthorized access. Potential threats are handled in a case-by-case manner with respect to risk level.

3.2 Granting Access to Oracle Administrative Accounts

Requirements

R4. Document the procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

Procedures

1. The IT account administrator receives an official access form from the director of data management requesting access for the Oracle administrative account user.

2. The director of data management verifies the user's identification.

3. An IT account administrator grants user access based on assigned privileges. **Note:** Privileges are assigned using the principle of least privilege.

4. The IT account administrator confirms access creation by signing the request form and returning it to the director.

3.3 Deactivating User Access & Updating Personnel Changes

Requirements

R4. Document the procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

R5. Update information system access no more than 5 business days after terminations and no more than 30 days after other personnel status changes. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:7,10)

R6. Review and/or revise user authorization upon notification of personnel status changes. The suggested parties responsible for notifications are system owners, managers, and human resources. (USG 3.1.1.3:8)

Procedures

1. To initiate and complete deactivation, the IT account administrator receives notification from the director of data management identifying the user whose access needs to be denied.

2. Immediately upon notification the IT account administrator:
   - Revokes all user privileges
   - Changes shared passwords
   - Records such action in the activity journal

Personnel Status Changes

1. Immediately after a personnel status change notification, the IT account administrator updates privileges to reflect the user’s new role.

3.4 Information System Access Review

Requirements

R4. Document the procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

R7. System owners will maintain an up-to-date mapping of users to information systems. IT account administrators will review user access information with system owners every **4 months**. (USG 3.1.1.3:3,9)

Procedures

1. IT account administrators review system access audits every 4 months.

2. The IT account administrator discusses needed modifications with the director of database administrators. The modifications are made upon director's request. In exceptional cases, the IT account administrator may need to make immediate modifications.

3. The IT account administrator documents the transaction in the activity journal.

Section 4: Xtender

4.1 Authenticating Access & Preventing Unauthorized Use

Requirements

R2. Ensure appropriate resources are available and maintained to adequately authenticate and verify authorized access. Resources appropriate for preventing and detecting unauthorized use shall be maintained. (USG 3.1.1.3:5b-c)

R3. Follow appropriate procedures to ensure only authorized users are allowed physical, electronic, or other access. **Note:** The system owners, IT account administrators, and users are all responsible for preventing unauthorized use. (USG 3.1.1.3:4,6)

Procedures

1. To authenticate access, Xtender uses IDs and passwords that are shared and synchronized with Banner.

2. Unauthorized access is detected through the IT account administrator's review of failed login attempts and investigation of unusual activity.

4.2 Granting User Access

Requirements

R4. Document the procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

Procedure

1. Upon receipt of an official access form signed by the system owner and ISO, the IT account administrator creates user access and sets permissions according to the principle of least privilege.

2. After the account is created, the user receives access information via email.

4.3 Deactivating User Access & Updating Personnel Changes

Requirements

R4. Document the procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

R5. Information system access will be updated no more than **5 business days** after terminations and no more than **30 days** after other personnel status changes. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:7,10)

R6. Review and/or revise user authorization upon notification of personnel status changes. The suggested parties responsible for notifications are system owners, managers, and human resources. (USG 3.1.1.3:8)

Procedures

1. The IT account administrator receives notification through EREQ, a weekly termination report, or information obtained from a system owner which triggers the termination of access.

2. Within 5 business days of notification the IT account administrator:
    - Locks the user's account
    - Removes all user privileges
    - Records such action in the activity journal

Personnel Status Changes

1. Within 5 business days of a personnel status change notification, the IT account administrator deactivates the account (per step 2 above). Updated access is granted when an official request is received (see Section 4.2).

4.4 Information System Access Review

Requirements

R4. Document the procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

R7. System owners will maintain an up-to-date mapping of users to information systems. IT account administrators will review user access information with system owners every **4 months**. (USG 3.1.1.3:3,9)

Procedures

1. The IT account administrator provides the system owner with a list of users that have access to their system every four months. However, an up-to-date list of user accounts is available upon request of the CIO.

2. The IT account administrator modifies user access at the system owner's request.

3. The system owner acknowledges the list has been reviewed and responds via email.

4. The IT account administrator documents the transaction in the activity journal.

Section 5: R25

Important:

The R25 system does not process or store confidential or sensitive information.

Administrative users are employees at Georgia College, and an IT account administrator will grant, review, and deactivate their access. Standard users can be Georgia College affiliates or anyone with access to the internet; for that reason, the R25 system does not require IT controls or a high level of access security with regard to standard users. Standard users are solely responsible for the creation and integrity of their access information. Deactivation, updates, and reviews are inapplicable. **Therefore, the following procedures will only apply to administrative users.**

5.1 Authenticating Access & Preventing Unauthorized Use

Requirements

R2. Ensure appropriate resources are available and maintained to adequately authenticate and verify authorized access. Resources appropriate for preventing and detecting unauthorized use shall be maintained. (USG 3.1.1.3:5b-c)

R3. Follow appropriate procedures to ensure only authorized users are allowed physical, electronic, or other access. Note: The system owners, IT account administrators, and users are all responsible for preventing unauthorized use. (USG 3.1.1.3:4,6)

Procedures

1. Only administrative users from the facilities reservations department and the office of the registrar need access to R25. User access is easily monitored.

2. Administrative user accounts are reviewed regularly.

5.2 Granting Administrative Access to R25

Requirements

R4. Document the procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7) (Continued)

Procedures

1. The IT account administrator receives a user access notification request from the manager of the facilities reservations department or the office of the registrar.

2. Upon notification, the IT account administrator assists users with creating a password. All administrative users are assigned the same permissions.

5.3 Deactivating User Access & Updating Personnel Changes

Requirements

R4. Document the procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

R5. Update information system access no more than 5 business days after terminations and no more than 30 days after other personnel status changes. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:7,10)

R6. Revise and/or review user authorization upon notification of personnel status changes. The suggested parties responsible for notifications are system owners, managers, and human resources. (USG 3.1.1.3:8)

Procedures

1. To initiate and complete deactivation, the IT account administrator receives notification through EREQ, a weekly termination report, or information obtained directly from the manager of the facilities reservations department or the office of the registrar.

2. Within **5** business days of notification the IT account administrator:
   - Removes privileges by adjusting account details
   - Records such action in the activity journal

Personnel Status Changes

1. Personnel status changes are received from the managers of facilities reservations or the office of the registrar and accounts are adjusted per step 5.2.

5.4 Information System Access Review

Requirements

R4. Document the procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

R7. System owners will maintain an up-to-date mapping of users to information systems. IT account administrators will review user access information with system owners every **4 months**. (USG 3.1.1.3:3,9)

Procedures

1. IT account administrator provides the facilities reservations department and the office of the registrar with a list of users that have access to their system every 4 months. However, an up-to-date list of user accounts is available upon request of the CIO.

Section 6: PeopleSoft Financials (PSFIN)

6.1 Authenticating Access & Preventing Unauthorized Use

Requirements

R2. Ensure appropriate resources are available and maintained to adequately authenticate and verify authorized access. Resources appropriate for preventing and detecting unauthorized use shall be maintained. (USG 3.1.1.3:5b-c)

R3. Follow appropriate procedures to ensure only authorized users are allowed physical, electronic, or other access. Note: The system owners, IT account administrators, and users are all responsible for preventing unauthorized use. (USG 3.1.1.3:4,6)

Procedures

1. A hierarchy of tacit and expressed communication is used to authenticate PSFIN users. Internal communication, segregated duties, and workflow are utilized to create a system of authentication.

2. Users must have a unique login ID and a new password must be generated every 120 days. Accounts are locked if multiple failed attempts occur.

3. PeopleSoft is only available while connected to the state internet service provider.

4. At least twice per academic year, the account administrator facilitates workshops covering PSFIN practices. Attendance is documented.

5. Once per academic year, the lead security administrator communicates with managers of customer users to ensure they under the access of their direct reports.

6. To prevent and detect unauthorized access, the PeopleSoft account administrator maintains a personal user access file that is compared to system generated audits. The PSFIN account administrator takes action adjusting roles and access as necessary.

6.2 Granting PeopleSoft Access

Requirements

R4. Document the procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

Procedures

1. Supervisors or users submit access requests are made via email or telephone.

2. Users receive ‘how to’ instructions via email to initiate and complete self-service process.

3. Users send the PSFIN account administrator login ID.

4. The PSFIN account administrator applies roles based on principle of least privilege.

5. The PSFIN account administrator confirms access with user and supervisor via email.

6. The PSFIN account administrator completes and mails a security request form (SRF) to the user and creates an entry in the security log reflecting the activity.

7. The user and supervisor sign and return the original SRF. Users are expected to a keep copy for their records.

6.3 Deactivating User Access & Updating Personnel Changes

Requirements

R4. Document the Procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

R5. Update information system access no more than 5 business days after terminations and no more than 30 days after other personnel status changes. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:7,10)

R6. Revise and/or review user authorization upon notification of personnel status changes. The suggested parties responsible for notifications are system owners, managers, and human resources. (USG 3.1.1.3:8)

Procedures

1. The PeopleSoft account administrator conducts a weekly review of local documentation and employment reports to determine users whose current employment parameters are equal to separation.

2. Upon notification the PeopleSoft account administrator:
   - Removes all roles, deactivates the user profile, and updates security forms

Personnel Status Changes

1. The user's manager notifies the PeopleSoft account administrator when personnel status changes occur.

2. The PeopleSoft account administrator modifies the account using the principle of least privilege.

3. If the user still requires access the new access information is emailed to the user's manager and the PeopleSoft account administrator updates security forms.

6.4 Information System Access Review

Requirements

R4. Document the Procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

R7. System owners will maintain an up-to-date mapping of users to information systems. IT account administrators will review user access information with system owners every **4 months**. (USG 3.1.1.3:3,9)

Procedures

1. Terminations are documented in the human resources system and compared to documentation maintained the PSFIN account administrator.

2. The PeopleSoft account administrator regularly reviews local documentation and employment reports to ensure only authorized users have access.

3. Issues found during the review are addressed immediately.

4. The PeopleSoft account administrator conducts an annual user review/attestation.

Section 7: ADP

7.1 Authenticating Access & Preventing Unauthorized Use

Requirements

R2. Ensure appropriate resources are available and maintained to adequately authenticate and verify authorized access. Resources appropriate for preventing and detecting unauthorized use shall be maintained. (USG 3.1.1.3:5b-c)

R3. Follow appropriate Procedures to ensure only authorized users are allowed physical, electronic, or other access. Note: The system owners, IT account administrators, and users are all responsible for preventing unauthorized use. (USG 3.1.1.3:4,6)

Procedures

1. Upon registration each user is assigned a unique logon ID and creates a password.

2. ADP users are authenticated by verification questions during the self-service registration process.

3. Users are prompted to create a specific password and to create a new password every 120 days.

4. Users with ‘practitioner’ status have digital certificates assigned to their operator profile and installed on their computer system.

5. Employee verifications, security questions, and lockouts prevent unauthorized access.

7.2 Granting ADP Access

Requirements

R4. Document the Procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

Procedures

1. The human resources personnel inputs the user's personal information into the ADP system.

2. The user receives necessary self-service access based on predefined employment groups.

3. Users receive email instructions on how to initiate and complete self-service registration.

4. The USG Shared Services Center creates class and adds practitioner based and adds the practitioner based on local security workbook.

5. The ADP account administrator and USG Shared Services center work together to install digital certificates on the computer system of users who require practitioner access.

7.3 Deactivating User Access & Updating Personnel Changes

Requirements

R4. Document the Procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

R5. Update information system access no more than 5 business days after terminations and no more than 30 days after other personnel status changes. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:7,10)

R6. Revise and/or review user authorization upon notification of personnel status changes. The suggested parties responsible for notifications are system owners, managers, and human resources. (USG 3.1.1.3:8)

Procedures

1. The ADP account administrator communicates with supervisors to determine whether or not a user is in the terminated class.

2. Non-practitioners have access to their personal information within the ADP system for 3 years post separation. After 3 years the account is deactivated.

7.4 Information System Access Review

Requirements

R4. Document the Procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

R7. System owners will maintain an up-to-date mapping of users to information systems. IT account administrators will review user access information with system owners every **4 months**. (USG 3.1.1.3:3,9)

Procedures

1. The USG Shared Services Center security administrator regularly reviews user access.

2. The USG Shared Services Center and the ADP account administrator conduct access reviews quarterly.

Section 8: Domain Access

8.1 Authenticating Access & Preventing Unauthorized Use

Requirements

R2. Ensure appropriate resources are available and maintained to adequately authenticate and verify authorized access. Resources appropriate for preventing and detecting unauthorized use shall be maintained. (USG 3.1.1.3:5b-c)

R3. Follow appropriate Procedures to ensure only authorized users are allowed physical, electronic, or other access. Note: The system owners, IT account administrators, and users are all responsible for preventing unauthorized use. (USG 3.1.1.3:4,6)

Procedures

1. Access requests are validated by Human Resources or Academic Affairs and Serve. All requests to the System Administrator are received and documented via the help ticket system.

2. To ensure the account does not already exist, the System Administrator investigates system information before user access is created.

3. All users are required to have a username and unique password.

4. The System Administrator group only acknowledges request filtered through EREQ or an approved channel e.g. an IT Account Administrator.

5. Level of access is reviewed and granted on a need basis. When a user requests any privilege increase a representative from their department must verify the validity of that request.

8.2 Granting Domain Access

Requirements

R4. Document the Procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

Procedures

1. The System Administrator receives an EREQ notification initiated by Human Resources or Academic Affairs and awaits confirmation from Serve via help ticket.

2. After receiving the help ticket from Serve, the System Administrator will ensure that the account does not already exist.

3. If necessary, the system administrator will create a domain account following the principle of least privilege.

4. The system administrator synchronizes the user’s password so that technicians can reference the initial password and help client directly.

8.3 Deactivating User Access & Updating Personnel Changes

Deactivation Procedures are based upon type of separation. System Administrators respond to deactivation request using the standards of amicable separations, non-amicable separations, and personnel changes.

Requirements

R4. Document the Procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

R5. Update information system access no more than 5 business days after terminations and no more than 30 days after other personnel status changes. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:7,10)

R6. Revise and/or review user authorization upon notification of personnel status changes. The suggested parties responsible for notifications are system owners, managers, and human resources. (USG 3.1.1.3:8)

Procedures

1. Deactivation following an amicable separation.
    - The System Administrator is notified by EREQ and a help ticket from Serve.
    - The System Administrator acknowledges the list of accounts requiring deactivation by placing them on a calendar.
    - Domain access is revoked within 1 business day of an amicable separation.

2. Deactivation following a non-amicable separation.
    - The System Administrator is notified by EREQ and by a 'flagged' help ticket or is contacted by a superior when user access must be revoked.
    - The System Administrator revokes account privileges **immediately**.

Personnel Status Changes

1. Deactivation following a personnel change.
    - The System Administrator acknowledges the change; however, users maintain domain access unless they are retirees.

8.4 Information System Access Review

Requirements

R4. Document the Procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

R7. System owners will maintain an up-to-date mapping of users to information systems. IT account administrators will review user access information with system owners every 4 months. (USG 3.1.1.3:3,9)

Procedures

1. The ticket system used to facilitate communication between Serve and the System Administrator group is the official method of documentation. The System Administrator complements this process by:

    - Regularly reviewing closed positions.
    - Auditing EREQ closures at random to ensure access has been deactivated.

Section 9: Email Access

9.1 Authenticating Access & Preventing Unauthorized Use

Requirements

R2. Ensure appropriate resources are available and maintained to adequately authenticate and verify authorized access. Resources appropriate for preventing and detecting unauthorized use shall be maintained. (USG 3.1.1.3:5b-c)

R3. Follow appropriate Procedures to ensure only authorized users are allowed physical, electronic, or other access. Note: The system owners, IT account administrators, and users are all responsible for preventing unauthorized use. (USG 3.1.1.3:4,6)

Procedures

1. Access requests are validated by Human Resources or Academic Affairs and Serve. All requests to the System Administrator are received and documented via the help ticket system.

2. To ensure the account does not already exist, the System Administrator investigates system information before user access is created.

3. All users are required to have a username and unique password.

4. The System Administrator group only acknowledges request filtered through EREQ or an approved channel e.g. an IT Account Administrator.

9.2 Granting Email Access

Requirements

R4. Document the Procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

Procedures

1. The System Administrator receives an EREQ notification initiated by Human Resources or Academic Affairs and awaits confirmation from Serve via help ticket.

2. After receiving the help ticket from Serve, the System Administrator will ensure that the account does not already exist and, if necessary, create an email account. **Note:** The principle of least privilege is not applicable to the email access process. All users have the same privilege level.

3. The System Administrator synchronizes the user’s password so that technicians can reference the initial password and help client directly.

9.3 Deactivating User Access & Updating Personnel Changes

Deactivation Procedures are based upon type of separation. System Administrators respond to deactivation request using the standards of amicable separations, non-amicable separations, and personnel changes.

Requirements

R4. Document the Procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

R5. Update information system access no more than 5 business days after terminations and no more than 30 days after other personnel status changes. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:7,10)

R6. Revise and/or review user authorization upon notification of personnel status changes. The suggested parties responsible for notifications are system owners, managers, and human resources. (USG 3.1.1.3:8)

Procedures

1. Deactivation following an amicable separation.
    - The System Administrator is notified by EREQ and a help ticket from Serve.
    - The System Administrator acknowledges the list of accounts requiring deactivation by placing them on a calendar.
    - Within 30 days of the separation, the System Administrator disables those accounts. After an additional 30 days the accounts are removed.

2. Deactivation following a non-amicable separation.
    - The system administrator is notified by EREQ and a help ticket from Serve that is ‘flagged’ or alerted by a superior to remove access.
    - The System Administrator revokes account privileges **immediately**.

Personnel Status Changes

1. Deactivation following a personnel change.
    - Typically, personnel changes do not prompt administrative action because there are no privilege levels.
    - Retirees may request to maintain email account access.

9.4 Information System Access Review

Requirements

R4. Document the Procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

R7. System owners will maintain an up-to-date mapping of users to information systems. IT account administrators will review user access information with system owners every 4 months. (USG 3.1.1.3:3,9)

Procedures

1. The ticket system used to facilitate communication between Serve and the System Administrator group is the official system of documentation. However, the System Administrator complements this process by:

    - Regularly reviewing closed positions.
    - Auditing EREQ closures at random to ensure access has been deactivated.

Section 10: Revize (Web Content Management System)

10.1 Authenticating Access & Preventing Unauthorized Use

Requirements

R2. Ensure appropriate resources are available and maintained to adequately authenticate and verify authorized access. Resources appropriate for preventing and detecting unauthorized use shall be maintained. (USG 3.1.1.3:5b-c)

R3. Follow appropriate Procedures to ensure only authorized users are allowed physical, electronic, or other access. Note: The system owners, IT account administrators, and users are all responsible for preventing unauthorized use. (USG 3.1.1.3:4,6)

Procedures

1. To prevent and detect unauthorized access accounts must be requested by a GC employee on behalf of their department or unit before granting access.
2. System owner/account administrator communicates with section supervisors every 4 months reaffirm approved users and grants, reviews, deactivates, updates, and/or terminates account access based upon that communication.
3. Usernames are categorized into two groups. Faculty and staff are titled "first name.last name, and students are "first name_last name".

10.2 Granting Revise Access

Requirements

R4. Document the Procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

Procedures

1. The system owner/account administrator receives notification via email, phone, or personal request from a section supervisor or Georgia College employee representing their department or unit.

2. The system owner/account administrator creates accounts and passwords within 24 hours of receiving a request. **Note:** Accounts are created with regard to the principle of least privilege.

3. The system owner/account administrator sends an email notification to the requesting Georgia College employee to confirm access has been granted and to dictate further instructions.

4. The user must contact the system owner/account administrator by phone or in person to receive their access password.

5. The system owner/account administrator records the transaction in an activity journal.

10.3 Deactivating User Access & Updating Personnel Changes

Requirements

R4. Document the Procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

R5. Update information system access no more than 5 business days after terminations and no more than 30 days after other personnel status changes. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:7,10)

R6. Revise and/or review user authorization upon notification of personnel status changes. The suggested parties responsible for notifications are system owners, managers, and human resources. (USG 3.1.1.3:8)

Procedures

1. To initiate and complete deactivation, the system owner/account administrator receives notification through EREQ, a termination report, or information obtained from a section supervisor.

2. Within **24** hours of notification the system owner/account administrator:

    - Deactivates the user’s account entirely

    - Records such actions in the activity journal

    - Emails the section supervisor to confirm deactivation

3. The system owner/account administrator documents the transaction in an activity journal.

10.4 Information System Access Review

Requirements

R4. Document the procedures used to grant, review, deactivate, update, and/or terminate account access. The system owner will ensure that user access is based on the principle of least privilege. (USG 3.1.1.3:5a,7)

R7. System owners will maintain an up-to-date mapping of users to information systems. IT account administrators will review user access information with system owners every **4** months. (USG 3.1.1.3:3,9)

Procedures

1. The system owner/account administrator provides the section supervisor with a list of users that have access to their system every 4 months. However, an up-to-date list of user accounts is available upon request.

2. The system owner/account administrator modifies user access at the section supervisor's request.

3. The system owner/account administrator acknowledges the list has been reviewed and responds via email.

4. The system owner/account administrator documents the transaction in the activity journal.