Gordon State College

User Account Management
Procedures

User Account Management

Table of Contents

Revisions

Original Date: October 4, 2013

Revision Number	Description	Date	Revised By
1	Added ExpressionEngine (Section 25)	11/12/2014	Troy Stout
2			
3			
4			
5			

Reviewed

Review Date	Reviewed By
10/4/2013	Troy Stout
1/15/2015	Troy Stout

Introduction

Gordon State College and the University System of Georgia (USG) recognize the importance of protecting our state's strategic IT assets. These assets must be protected from unauthorized access, loss, contamination, or destruction (BoR IT Handbook 3.1.1). Proper management and protection of an IT asset is characterized by ensuring the confidentiality, integrity, and availability of the system. Establishing guidelines and preventative controls for managing user access in a continual and consistent manner is critical in order to lower risks that could negatively impact the institution or USG as a whole. Effective use and the protection of information systems/resources is a shared responsibility among all individuals at the institution (functional owners, administrators, approvers, and users). This document outlines acceptable user account management procedures and is in accordance with USG policies/procedures and other applicable Gordon State College guidelines.

Purpose

Information Systems require a degree of protection commensurate with their value. The following procedures address user account management for information systems including initial user access authorizations, access reviews, updates/transfers, and termination procedures. User access must be based on the *Principle of Least Privilege* meaning that user access is restricted to what is necessary to perform his or her job.

Scope

These procedures **must** be followed by all Gordon State College administrators, faculty, staff, students, contractors, guests and any other individuals who use the College's information systems from any location.

Terms and Definitions

Sensitive – a system is defined as sensitive when having any combination of the following data characteristics:

1. Social Security Account Numbers
2. Personal identification numbers which may be used other than Social Security Number
3. Information protected by federal, state or local laws, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Family Educational Rights and Privacy Act (FERPA), etc.
4. Credit card account numbers
5. Bank account numbers
6. Contains critical infrastructure information (Floor plans, system passwords, IT system configurations/infrastructure)
7. Loss of confidentiality or integrity will cause significant harm to the institution and/or individual

Critical – a system is defined as critical when having any combination of the following characteristics:

- Prolonged loss of availability could prevent college from achieving organizational goals and objectives
- Loss of availability may create safety and/or security risk
- Availability mandated by federal, state or local laws

Account Administrator – individual(s) that implement authentication and enforce access rights approved by the system owner for an IT asset.

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.

System Owner – 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 – individuals who use the information processed by an IT asset. Users can be used synonymously with the word *employee*.

Hosted – a computer system and/or application service owned and operated by an external service provider and makes the system available to remote clients, usually over the Internet.

Requirements

[R1] Identify and classify information systems that process or store confidential or sensitive information, or are critical systems and document the owner for each of these systems. A list of systems and individuals identified as owners will be maintained and made available upon request. (BoR IT Handbook 3.1.1.3:1,2)

[R2] Maintain an up-to-date mapping of users to information systems. At a minimum, the account administrator will provide the system owner with user access information for assessment every **four (4)** months. All findings will be documented with the Information Technology Department. (BoR IT Handbook 3.1.1.3:3,9)

[R3] Ensure only authorized users are allowed physical, electronic, or other access to Information systems. The system owners, account administrators, and users share the responsibility of preventing unauthorized access to IT assets. (BoR IT Handbook 3.1.1.3:4,6)

[R4] Document procedures to grant, review, deactivate, update, and/or terminate account access. The system owners will analyze user roles and determine the appropriate level of access based on job requirements. User access will be based on the *principle of least privilege*. (BoR IT Handbook 3.1.1.3:5a,7)

[R5] 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. (BoR IT Handbook 3.1.1.3:5b-c)

[R6] User authorization must be reviewed and revised by the system owner upon notification of personnel status changes in job function, status, transfers, referral privileges, and/or affiliation. The suggested responsible parties for notifications are system owners, managers, and Human Resources. (BoR IT Handbook 3.1.1.3:8)

[R7] Update system access no more than **five (5)** business days after terminations and no more than **thirty (30)** days after other personnel status changes. (BoR IT Handbook 3.1.1.3:10)

Section 1: Maintaining Systems Inventory/Classification

Requirements	Procedures
[R1]	Gordon State College maintains an inventory list of all systems. The list contains the following: system name, purpose, system owner, main users, criticality and sensitivity classification, risk categorization, and other system details. This list is readily available upon request to the Director of Information Technology.

Section 2: Banner

Banner is the name of a fully integrated software solution developed by Ellucian (formerly Sungard Higher Education) and used by the college to manage its business operations. The Banner system supports and manages student information, accounts receivable, and financial aid.

2.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	1. Each department will protect information resources in Banner by adopting and implementing the user access standards set forth in this document. 2. System owners and supervisors will inform prospective users about the importance of keeping their access information safe. 3. Account administrator will ensure unique identification of each user and assignment of access privileges. 4. Users are required to create a specific unique password after they login with the account information provided to them at initial setup, and to create a new password every 122 days with a 10 day grace period. 5. Accounts are locked after 5 unsuccessful attempts. 6. System owners communicate with account administrators through a help desk system to identify and document approved users and to grant, review, deactivate, update, and/or terminate account access based upon that communication. 7. To prevent and detect unauthorized use, account administrators monitor logs generated by the Banner system. Locked accounts are reviewed periodically and unusual activity is investigated by Information Technology. Potential threats are handled on a case-by-case basis with respect to risk level. 8. Remote access to the system is only permitted through secure, authenticated, and centrally managed access methods (e.g. VPN). 9. System administrators routinely require “privileged” access to the Banner system to perform essential system administration functions. The number of privileged accounts must be kept to a minimum and only provided to those individuals knowledgeable about the IT used in the system and whose job duties require it. 10. Environmental safeguards are used for controlling physical access to equipment and data rooms. Only a limited number of personnel will have physical access to the data center including Information Technology personnel, maintenance personnel, Public Safety and key administrators.

2.2 Granting Banner Access

Requirements	Procedures
[R4]	1. For a new hire, Human Resources emails the new user's direct supervisor (cc's Information Technology) relevant employment information along with a link to an electronic access request form. 2. The user's direct supervisor must complete and submit the *Computer Access Form – New Employee* online to initiate account creation, assign Banner form privileges, and determine what level of access is allowed (i.e. query and/or modify). Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 3. If the direct supervisor has not been identified as a system owner for a Banner form(s) requested, the system owner of the form(s) is contacted by the account administrator and approval is substantiated before access is granted. Access privileges should be commensurate with the user's defined responsibilities. 4. The account administrator creates account access after receiving proper approval from the system owner. 5. The user's supervisor receives account information from the account administrator after the account has been created. Note: appropriate permissions assigned to the account – taking into consideration the principle of least privilege and separation of duties – is the responsibility of both the supervisor and the system owner. 6. The supervisor will distribute account information to the new user and verify the temporary password has been changed. 7. Communication between Human Resources, system owners, supervisors, and account administrators will be documented via the help desk ticketing system.

2.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** 1. Human Resources is notified of an employee's pending termination and/or need for account deactivation. 2. To officially initiate user account deactivation, Human Resources will send the user's direct supervisor (cc's Information Technology) an email with a link to an electronic termination request form. 3. The user's direct supervisor must complete and submit the *Computer Access Form – Employee Terminated Checklist* online. 4. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Within **five (5)** business days* of form submission the account administrator will: • Remove all user privileges • Deactivate the user's account • Document completion and notify employee's supervisor and Human Resources * when an employee is terminated for cause, account deactivation must occur immediately. **Personnel Status Changes** 1. For changes to existing user accounts not within the scope of termination/deactivation, a *Computer Access Form - Change Employee Access* form must be completed by the user's direct supervisor. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 2. If the direct supervisor has not been identified as a system owner for any additional system privileges requested, the appropriate system owner is contacted by the account administrator and approval is substantiated before any additional access is granted. Access privileges should be commensurate with the user's defined responsibilities. 3. To maintain the requirements of least privilege, when a user transfers to a new role and/or department, all privileges should first be removed and then new privileges added that are required in the user's new role. 4. Within **thirty (30)** days of user status changes the account administrator will: • Remove user privileges (if applicable) • Update system access • Document changes and notify employee's supervisor

2.4 User Access Review

Requirements	Procedures
[R2] [R4]	1. The account administrator provides each system owner a list of users that have access to forms within their specific module in Banner every **four (4)** months (i.e. modules *Finance*, *Financial Aid*, *Student*, and *General*). An up-to-date list of users is also available upon request. 2. A user access list is submitted by the account administrator to the system owner for review via the help desk ticketing system. A system owner acknowledges the list has been reviewed by responding to the ticket via email and requests any changes, if applicable. 3. The account administrator modifies user access and the system owner is notified. 4. The account administrator documents the entire transaction in the help desk ticketing system. 5. System owners are assigned a **one (1)** month time frame to complete the user access review. 6. A status report is submitted to the Vice President of Business Affairs following the allotted time frame.

Section 3: Banner Web

Banner includes a number of web-based features so that students, faculty, advisors, and staff can conveniently access personalized college services online.

3.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	1. Faculty, staff and students are trained on how to login and change access information to Banner Web during onboarding/orientation sessions. Officials leading orientation sessions will stress the importance of keeping access information safe. 2. Unique account credentials are created for all faculty, staff, and students. 3. Students are required to create a new PIN by answering a predefined security question during initial setup. Faculty and staff are required to create a security question and reset their PIN after they login with the account information provided to them at initial setup. 4. PINs expire every 2 years based on Banner baseline. 5. A Banner Web session will timeout after 30 minutes of inactivity, requiring re-authentication. 6. Faculty must be teaching in the current or a future term in order to login to Banner Web. 7. To prevent and detect unauthorized use, account administrators monitor logs generated by the Banner system. Unusual activity is investigated by Information Technology. 8. System administrators routinely require “privileged” access to the Banner system to perform essential system administration functions. The number of privileged accounts must be kept to a minimum and only provided to those individuals knowledgeable about the IT used in the system and whose job duties require it. 9. Environmental safeguards are used for controlling physical access to equipment and data rooms. Only a limited number of personnel will have physical access to the data center including Information Technology personnel, maintenance personnel, Public Safety and key administrators.

3.2 Granting Banner Web Access

Requirements	Procedures
[R4]	**Students** 1. The admissions personnel input student enrollment data into the Banner system. 2. The system uses the information to generate a GCID and create a record in the Banner Web user table. 3. Students are trained on how to login and change access information to Banner Web during orientation sessions. Students also receive an enrollment packet with instructions on how to initiate access. **Faculty** 1. For a new faculty hire, Human Resources emails Academic Affairs relevant employment information where Academic Affairs will then input that data into the Banner system and generate a GCID. 2. Academic Affairs must complete and submit the *Computer Access - New Faculty Form* online to initiate Banner Web access. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 3. The account administrator creates a record for the user in the Banner Web user table. Faculty are assigned access at the lowest level of the principle of least privilege. 4. The faculty member's assigned academic department receives account information from the account administrator after the account has been created. PINs are expired upon initial logon and must be changed by the user. 5. The department administrative assistant will distribute account information to the faculty member and verify the temporary password has been changed. **Staff** 1. For a new staff hire, Human Resource personnel input employment data into the Banner system and generate a GCID. 2. Human Resources emails the new user's direct supervisor (cc's Information Technology) relevant employment information along with a link to an electronic access request form. 3. The user's direct supervisor must complete and submit the *Computer Access Form – New Employee* online to initiate account creation. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 4. The account administrator creates a record for the user in the Banner Web user table. Staff are assigned access at the lowest level of the principle of least privilege in Banner Web. PINs are expired upon initial logon and must be changed by the user. 5. Any additional access in Banner Web must be communicated to the account administrator by the user's direct supervisor. Additional access privileges

	available in Banner Web is minimal and should be commensurate with the user's defined responsibilities. 6. The user's supervisor receives account information from the account administrator after the account has been created. 7. The supervisor will distribute account information to the new user and verify the temporary password has been changed. 8. Communication between Human Resources, supervisors, and account administrators will be documented via the help desk ticketing system.

3.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** Students Student accounts are **never** terminated /deactivated. Student accounts are available to them indefinitely as it has important information concerning past academic records. Faculty/Staff 1. Human Resources is notified of an employee's pending termination and/or need for account deactivation. 2. To officially initiate user account deactivation, Human Resources will send the user's direct supervisor (cc's Information Technology) an email with a link to an electronic termination request form. 3. The user's direct supervisor must complete and submit the *Computer Access Form – Employee Terminated Checklist* online. 4. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Within **five (5)** business days* of form submission the account administrator will: • Deactivate the user's account • Document completion and notify employee's supervisor and Human Resources * when an employee is terminated for cause, account deactivation must occur immediately. **Personnel Status Changes** 1. Updates concerning terminations and personnel status changes are not applicable to student accounts. 2. Most faculty and staff are assigned access at the lowest level of the principle of least privilege therefore; personnel status changes requiring system privilege updates are uncommon. Personnel status changes are reviewed on a case-by-case basis by the account administrator.

3.4 User Access Review

Requirements	Procedures
[R2] [R4]	**Students** Student accounts do not require review because access is neither terminated nor updated. **Faculty and Staff** Most faculty and staff are assigned access at the lowest level of the principle of least privilege and, therefore, do not require periodic review.

Section 4: Oracle Administrative (DBMS) Accounts

4.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	1. System administrators routinely require "privileged" access to the Oracle database to perform essential system administration functions. The number of privileged accounts must be kept to a minimum and only provided to those individuals knowledgeable about the IT used in the system and whose job duties require it. 2. The database administrator uses internal communication to identify approved users and maintains shared account credentials. 3. To prevent and detect unauthorized use, the database and network administrators monitor logs generated by the DBMS and other internal systems. Any unusual activity is investigated by Information Technology. Potential threats are handled on a case-by-case basis with respect to risk level. 4. Oracle accounts are locked after 5 unsuccessful attempts. 5. Remote access to the system is only permitted through secure, authenticated, and centrally managed access methods (e.g. VPN). 6. Environmental safeguards are used for controlling physical access to equipment and data rooms. Only a limited number of personnel will have physical access to the data center including Information Technology personnel, maintenance personnel, Public Safety and key administrators.

4.2 Granting Access to Oracle Administrative Accounts

Requirements	Procedures
[R4]	1. The database administrator receives an official request from the Director of Information Technology on behalf of an employee requesting access to an Oracle administrative account. 2. Database administrator verifies access privileges requested are commensurate with the prospective user's defined responsibilities. 3. The database administrator will distribute account information to the new user and inform the user that the account should only be used for essential system administration functions.

4.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** 1. The database administrator receives notification from the Director of Information Technology identifying the user whose access to Oracle administrative accounts should be revoked. 2. Immediately upon notification the database administrator will: • Remove user privileges (if applicable) • Change shared passwords • Document via the help desk ticketing system. **Personnel Status Changes** Immediately upon notification of a personnel status change the database administrator will: • Remove user privileges (if applicable) • Change shared passwords • Document via the help desk ticketing system.

4.4 User Access Review

Requirements	Procedures
[R2] [R4]	1. The database administrator reviews Oracle administrative accounts every **four (4)** months. 2. The database administrator discusses needed modifications with the Director of Information Technology. The modifications can be made upon the Director's request. In some circumstances, the database administrator may need to make immediate modifications. 3. The database administrator documents the process in the help desk ticketing system.

Section 5: Banner Document Management System (BDMS)

Banner Document Management System (BDMS) is part of Ellucian and used by the college to scan, index, and view electronic documents. BDMS can be accessed from within forms in Banner or via a web interface.

5.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	To authenticate access, BDMS user accounts are synchronized from Banner. See Section 1.1 under Banner for authentication and authorized access mechanisms and processes.

5.2 Granting User Access

Requirements	Procedures
[R4]	1. For a new hire, Human Resources emails the new user's direct supervisor (cc's Information Technology) relevant employment information along with a link to an electronic access request form. 2. The user's direct supervisor must complete and submit the *Computer Access Form – New Employee* online to initiate account creation and determine what security / application group access is required. A Banner user account must be setup first before BDMS access can be granted (see section 1.2). Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 3. If the direct supervisor has not been identified as a system owner for specific application groups in BDMS, the system owner of the application group is contacted by the account administrator and approval is substantiated before access is granted. Access privileges should be commensurate with the user's defined responsibilities. 4. The account administrator creates the account by importing the user from the Banner system after receiving proper approval from the system owner. 5. The user's supervisor receives notification from the account administrator that the account has been created. Note: appropriate application groups assigned to the account – taking into consideration the principle of least privilege – is the responsibility of both the supervisor and the system owner. 6. The user has access to BDMS from within forms in Banner or via a web interface. 7. Communication between Human Resources, system owners, supervisors, and account administrators will be documented via the help desk ticketing system.

5.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** 1. Human Resources is notified of an employee's pending termination and/or need for account deactivation. 2. To officially initiate user account deactivation, Human Resources will send the user's direct supervisor (cc's Information Technology) an email with a link to an electronic termination request form. 3. The user's direct supervisor must complete and submit the *Computer Access Form – Employee Terminated Checklist* online. 4. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Within **five (5)** business days* of form submission the account administrator will: • Remove all user privileges • Deactivate the user's account • Document completion and notify employee's supervisor and Human Resources * when an employee is terminated for cause, account deactivation must occur immediately. **Personnel Status Changes** 1. For changes to existing user accounts not within the scope of termination/deactivation, a *Computer Access Form - Change Employee Access* form must be completed by the user's direct supervisor. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 2. If the direct supervisor has not been identified as a system owner for an application group requested, the appropriate system owner is contacted by the account administrator and approval is substantiated before any additional access is granted. Access privileges should be commensurate with the user's defined responsibilities. 3. To maintain the requirements of least privilege, when a user transfers to a new role and/or department, all privileges should first be removed and then new privileges added that are required in the user's new role. 4. Within **thirty (30)** days of user status changes the account administrator will: • Remove user privileges (if applicable) • Update application group access • Document changes and notify employee's supervisor

5.4 User Access Review

Requirements	Procedures
[R2] [R4]	1. The account administrator provides each system owner with a list of users that have access to their application group(s) every **four (4)** months. An up-to-date list of users is also available upon request. 2. A user access list is submitted by the account administrator to the system owner for review via the help desk ticketing system. A system owner acknowledges the list has been reviewed by responding to the ticket via email and requests any changes, if applicable. 3. The account administrator modifies user access and the system owner is notified. 4. The account administrator documents the entire transaction in the help desk ticketing system. 5. System owners are assigned a **one (1)** month time frame to complete the user access review. 6. A status report is submitted to the Vice President of Business Affairs following the allotted time frame.

Section 6: PeopleSoft Financials (PSFIN)

The PeopleSoft Financials system is an Information Technology Services (ITS) hosted database that contains the financial information for the institution. This includes *Travel & Expense (Employee Self-Service)* and *eProcurement* modules. There are three different types of users: Core users, eProcurement users, and Travel and Expense users.

6.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	1. Each department will protect information resources in PeopleSoft by adopting and implementing the user access standards set forth in this document. 2. System owners and supervisors will inform prospective users about the importance of keeping their access information safe. 3. Internal communications, mitigating controls for segregation of duties, and well-defined workflows are all utilized to verify authorized access and protect resources. 4. System reports are available in PeopleSoft that enable internal review of segregation of duties and terminated users. 5. Account administrator will ensure unique identification of each user and assignment of access privileges. 6. PeopleSoft is only accessible when connected to the PeachNet Internet Service Provider. 7. Users are required to create a specific unique password after initial setup, and to create a new password every 180 days with a 5 day grace period. 8. Accounts are locked after 5 unsuccessful attempts. 9. System owners communicate with account administrators through a help desk system to identify and document approved users and to grant, review, deactivate, update, and/or terminate account access based upon that communication.

6.2 Granting PeopleSoft Access

Requirements	Procedures
[R4]	**Travel and Expense Users (Employee Self-Service)** Travel and Expense users create their own account via a web portal*. All employees receive 'how to' instructions from Human Resources to initiate and complete the self-service registration process. * The account administrator will setup the account if it is determined that the new user will also be a Core PeopleSoft user (see Core and eProcurement Users). Core users do not have to go through the self-registration process. **Core and eProcurement Users** 1. For a new hire, Human Resources emails the new user's direct supervisor (cc's Information Technology) relevant employment information along with a link to an electronic access request form. 2. The user's direct supervisor must complete and submit the *Computer Access Form – New Employee* online to initiate account creation and determine what PeopleSoft roles are required. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 3. If the direct supervisor has not been identified as the system owner for PeopleSoft, the system owner is contacted by the account administrator and approval is substantiated before access is granted. Access privileges should be commensurate with the user's defined responsibilities. 4. The account administrator creates account access after receiving proper approval from the system owner. 5. The user's supervisor receives account information from the account administrator after the account has been created. Note: appropriate permissions assigned to the account – taking into consideration the principle of least privilege and separation of duties – is the responsibility of both the supervisor and the system owner. 6. The supervisor will distribute account information to the new user and verify the temporary password has been changed. 7. Communication between Human Resources, system owners, supervisors, and account administrators will be documented via the help desk ticketing system.

6.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** 1. Human Resources is notified of an employee's pending termination and/or need for account deactivation. 2. To officially initiate user account deactivation, Human Resources will send the user's direct supervisor (cc's Information Technology) an email with a link to an electronic termination request form. 3. The user's direct supervisor must complete and submit the *Computer Access Form – Employee Terminated Checklist* online. 4. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Within **five (5)** business days* of form submission the account administrator will: • Remove all user roles (core and eProcurement) • Deactivate the user profile • Document completion and notify employee's supervisor and Human Resources * when an employee is terminated for cause, account deactivation must occur immediately. **Personnel Status Changes** 1. For changes to existing user accounts not within the scope of termination/deactivation, a *Computer Access Form - Change Employee Access* form must be completed by the user's direct supervisor. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 2. If the direct supervisor has not been identified as a system owner for PeopleSoft, the appropriate system owner is contacted by the account administrator and approval is substantiated before any additional access is granted. Access privileges should be commensurate with the user's defined responsibilities. 3. To maintain the requirements of least privilege, when a user transfers to a new role and/or department, all roles should first be removed and then new roles added that are required in the user's new position. 4. Within **thirty (30)** days of user status changes the account administrator will: • Remove user roles (if applicable) • Update system access • Document changes and notify employee's supervisor

6.4 User Access Review

Requirements	Procedures
[R2] [R4]	1. The PeopleSoft account administrator runs a terminated users report each month and ensures only authorized users have access to the system. A user account is terminated immediately if an issue is found. 2. The account administrator provides the system owner a list of users and associated roles every **four (4)** months (Core and eProcurement). An up-to-date list of users is also available upon request. 3. A user access list is submitted by the account administrator to the system owner for review via the help desk ticketing system. A system owner acknowledges the list has been reviewed by responding to the ticket via email and requests any changes, if applicable. 4. The system owner will run the segregation of duties report and request adjustments as needed. 5. The account administrator modifies user access and the system owner is notified. 6. The account administrator documents the entire transaction in the help desk ticketing system. 7. System owners are assigned a **one (1)** month time frame to complete the user access review. 8. A status report is submitted to the Vice President of Business Affairs following the allotted time frame.

Section 7: ADP

ADP is a hosted database used by colleges and universities within the University System of Georgia for administrative functions such for time/labor management, payroll processing, accounts payable, and benefits.

There are two main types of user accounts within ADP, self-service portal users (all employees) and Ev5 users (practitioners).

7.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	1. The institution will protect information resources in ADP by adopting and implementing the user access standards set forth in this document. 2. System owners and supervisors will inform all employees about the importance of keeping their access information safe. 3. ADP account passwords are created by the employee during portal registration. Upon registration each user is assigned a unique logon ID and chooses a password. 4. ADP users are authenticated by employee verification questions during the self-registration process. 5. Users are required to create a specific unique password after initial registration, and to create a new password every 90 days. Users can not choose any of their last five (5) previously used passwords. 6. Accounts are locked after 3 unsuccessful or failed logon attempts for duration of 15 minutes. Users with 'practitioner' status are locked out permanently until the password is reset by Shared Services. 7. Temporary passwords, following a reset, are sent directly to the user's email account on record in ADP. These passwords expire after 24 hours. 8. ADP uses two-factor authentication for users with 'practitioner' status. Practitioners are required to "register" a workstation in order to login using their assigned credentials. Registration requires that the user receive a unique access code via e-mail that must then be input into a web form from his or her primary workstation. 9. System owners communicate with account administrators through a help desk system to identify and document approved users with 'practitioner' status and to grant, review, deactivate, update, and/or terminate account access based upon that communication.

7.2 Granting ADP Access

Requirements	Procedures
[R4]	1. On the employee's hire date, Human resources personnel input the user's personal employment information into the ADP system. 2. The user receives necessary self-service access based on predefined job types setup by Human Resources. 3. After the user has been added to the system, they are provided 'how to' instructions to initiate and complete the self-service registration process. 4. For a new hire, Human Resources emails the new user's direct supervisor (cc's Information Technology) relevant employment information along with a link to an electronic access request form. 5. The user's direct supervisor must complete and submit the *Computer Access Form – New Employee* online to initiate Ev5 administrative (practitioner) access, if applicable. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 6. If the direct supervisor has not been identified as a system owner for ADP, the system owner is contacted by the account administrator and approval is substantiated before the account provision process is continued. 7. The local account administrator will work with the system owner and the user's direct supervisor to determine the proper level of access based on the institution's security class master template. Access privileges should be commensurate with the user's defined responsibilities. 8. A user in Ev5 is assigned to one operator class from the class master. After consulting with the user's supervisor, if there is not an existing operator class that will accommodate the access needed for the new employee the following procedure is followed: i. The local account administrator enters a new class in the class master spreadsheet including the level of access required within each panel/task (i.e. view, update, or correction). Name of new class must include the Institution code (USG760) at the beginning of the class name. ii. Any additions or modifications made to the institution's class master are noted in bold red type. iii. The local account administrator will place the updated institution class master on the Shared Services FTP Server. 9. The local account administrator will enter all details related to the user's security, including the assigned operator class from the class master, into the security workbook template as a row entry. The security workbook is placed on the Shared Services FTP Server. Note: appropriate permissions assigned to the account – taking into consideration the principle of least privilege and separation of duties – is the responsibility of both the supervisor and the system owner. 10. The local account administrator submits a support ticket via e-mail to the USG Shared Services Center. 11. The USG Shared Services Center account administrator adds practitioner to a new or existing operator class based on local security workbook and security class master.

	12. The user receives account information from the USG Shared Services Center after the account has been created. 13. Communication between Human Resources, system owners, supervisors, the USG Shared Service Center and local account administrators will be documented via the help desk ticketing system.

7.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** Ev5 administrative (practitioner) users 1. Human Resources is notified of an employee's pending termination and/or need for account deactivation. 2. To officially initiate user account deactivation, Human Resources will send the user's direct supervisor (cc's Information Technology) an email with a link to an electronic termination request form. 3. The user's direct supervisor must complete and submit the *Computer Access Form – Employee Terminated Checklist* online. 4. Form submissions are sent directly to the helpdesk system and are reviewed by the local account administrator. Within **five (5)** business days of form submission: • The local account administrator will update the institution's security workbook template by assigning an operator class of USG###TERMINATED to the user. • The local account administrator will place the updated security workbook on the Shared Services FTP Server and submit a support ticket via e-mail notifying them of the termination. • The USG Shared Services Center account administrator will deactivate the user's account and send confirmation. • The local account administrator will document completion and notify employee's supervisor and Human Resources. Self-service portal users (all employees) Employees are terminated in ADP by Human Resources on or before (with a future effective date) the separation date. Former employees do retain access to ADP Self Service in order to view paycheck stubs and W2 information. **Personnel Status Changes** 1. For changes to existing user accounts not within the scope of termination/deactivation, a *Computer Access Form - Change Employee Access* form must be completed by the user's direct supervisor. Form submissions are sent directly to the helpdesk system and are reviewed by the account

	administrator(s). Requests by phone or email are not acceptable. 2. If the direct supervisor has not been identified as a system owner, the appropriate system owner is contacted by the account administrator and approval is substantiated before any additional access is granted. Access privileges should be commensurate with the user's defined responsibilities. 3. Within **thirty (30)** days of user status changes: • The local account administrator will update the institution's security workbook template and assign the user to a new or existing operator class. Existing operator class(es) are also updated in the local class master if necessary. • The local account administrator will place the updated security workbook and class master (if applicable) on the Shared Services FTP Server and submit a support ticket via e-mail notifying them of the change request. • The USG Shared Services Center account administrator will update user privileges based on local security workbook/class master and send confirmation. • The local account administrator will document completion and notify employee's supervisor.

7.4 User Access Review

Requirements	Procedures
[R2] [R4]	1. The USG Shared Services Center account administrator regularly reviews user access and sends reconciliation reports to institutions quarterly. 2. The local account administrator provides the system owner a list of Ev5 administrative (practitioner) users and operator classes every **four (4)** months. An up-to-date list of users is also available upon request. 3. A user access list is submitted by the account administrator to the system owner for review via the help desk ticketing system. A system owner acknowledges the list has been reviewed by responding to the ticket via email and requests any changes, if applicable. 4. The account administrator updates the local security workbook and class master. 5. The account administrator submits all changes to the USG Shared Services Center. 6. The USG Shared Services Center account administrator will update user privileges based on local security workbook/class master and send confirmation. 7. The account administrator documents the entire transaction in the help desk ticketing system. 8. System owners are assigned a **one (1)** month time frame to complete the user access review. 9. A status report is submitted to the Vice President of Business Affairs following the allotted time frame.

Section 8: Domain Access

A domain is a group of network resources (user accounts, computers, printers and other security principals) that are registered and administered within a central database (i.e. Active Directory service). All faculty, staff and students are provided a domain account and e-mail address. User access to the domain requires authentication to the campus Active Directory. Once authenticated, users may access network/server resources, e-mail and the Internet.

8.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	1. Each department will protect information resources on the Gordon State College network by adopting and implementing the user access standards set forth in this document. 2. System owners and supervisors will inform prospective users about the importance of keeping their access information safe. 3. Account administrator will ensure unique identification of each user and assignment of access privileges. 4. Users are required to create a specific unique password after they login with the account information provided to them at initial setup, and to create a new password every 122 days. 5. Accounts are locked after 5 unsuccessful logon attempts for duration of five (5) minutes. 6. System owners communicate with account administrators through a help desk system to identify and document approved users and to grant, review, deactivate, update, and/or terminate account access based upon that communication. 7. To prevent and detect unauthorized use, system administrators monitor network and server logs regularly. Unusual activity is investigated by Information Technology. Potential threats are handled on a case-by-case basis with respect to risk level. 8. Remote access to the domain is only permitted through secure, authenticated, and centrally managed access methods (e.g. VPN). 9. System administrators routinely require “privileged” access to the domain to perform essential system administration functions. The number of privileged accounts must be kept to a minimum and only provided to those individuals knowledgeable about the IT used in the system and whose job duties require it. 10. Environmental safeguards are used for controlling physical access to equipment and data rooms. Only a limited number of personnel will have physical access to the data center including Information Technology personnel, maintenance personnel, Public Safety and key administrators.

8.2 Granting Domain Access

Requirements	Procedures
[R4]	1. For a new staff hire, Human Resources personnel emails the new user's direct supervisor (cc's Information Technology) relevant employment information along with a link to an electronic access request form. 2. The user's direct supervisor must complete and submit the *Computer Access Form – New Employee* online to initiate domain account creation. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 3. For a new faculty hire, Academic Affairs personnel submits the *Computer Access Form – New Faculty Computer Access* online to initiate domain account creation. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 4. The account administrator creates domain account access. Users are assigned to AD groups based on department and/or job function following the principle of least privilege. These groups allow specific access to network resources. 5. E-mail accounts are provisioned at the same time and are associated with a user's domain account. **Note:** The principle of least privilege is not applicable to the e-mail provisioning process. All users have the same privilege level. 6. The user's supervisor or administrative assistant receives account information from the account administrator after the account has been created. 7. The supervisor or administrative assistant will distribute account information to the new user and verify the temporary password has been changed by the user. 8. Communication between Human Resources, Academic Affairs, supervisors, and account administrators will be documented via the help desk ticketing system.

8.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** 1. Human Resources is notified of an employee's pending termination and/or need for account deactivation. 2. To officially initiate user account deactivation, Human Resources will send the user's direct supervisor (cc's Information Technology) an email with a link to an electronic termination request form. 3. The user's direct supervisor must complete and submit the *Computer Access Form – Employee Terminated Checklist* online. Supervisors are encouraged to submit forms at least **three (3)** business days prior to the date of separation. 4. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Within **five (5)** business days* of form submission the account administrator will: • Remove user from all AD groups • Deactivate the user's account • Document completion and notify employee's supervisor and Human Resources 5. The system administrator will purge all deactivated domain and e-mail accounts on a quarterly basis. * when an employee is terminated for cause, domain account deactivation must occur immediately. **Personnel Status Changes** 1. For changes to existing domain accounts not within the scope of termination/deactivation, a *Computer Access Form - Change Employee Access* form must be completed by the user's direct supervisor. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 2. Level of access to network resources is granted on a need basis. Access privileges should be commensurate with the user's defined responsibilities. 3. To maintain the requirements of least privilege, when a user transfers to a new role and/or department, all AD group membership should first be removed and then new group privileges assigned that are required in the user's new role. 4. Within **thirty (30)** days of user status changes the account administrator will: • Remove group membership (if applicable) • Update network resource access • Document changes and notify employee's supervisor Note: Retirees maintain domain/e-mail access. Account administrator will remove all AD group membership following separation.

8.4 User Access Review

Requirements	Procedures
[R2] [R4]	1. Account administrator provides supervisors and/or department heads a list of domain users under their department every **four (4)** months. 2. The help desk ticketing system is used to document communication between the account administrator and supervisors/department heads. 3. Supervisors/Department heads are assigned a **one (1)** month time frame to complete the domain user review. 4. A status report is submitted to the Vice President of Business Affairs following the allotted time frame. 5. To complement the four month reviews the account/system administrator: • runs a terminated users report each month and ensures only authorized users have domain access. A user account is deactivated immediately if an issue is found. • audits domain accounts at random to ensure access is appropriate.

Section 9: Lenel OnGuard

OnGuard is a fully integrated ID management software solution developed by Lenel Systems for enrolling and producing employee and student ID credentials. OnGuard is also used for building and room access control.

9.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	1. Each department will protect information resources in Lenel OnGuard by adopting and implementing the user access standards set forth in this document. 2. System owners and supervisors will inform prospective users about the importance of keeping their access information safe. 3. Account administrator will ensure unique identification of each user and assignment of access privileges. 4. To authenticate access, a Lenel OnGuard user account is configured for single sign-on by synchronizing with a Domain account. The same user access controls for Domain accounts apply. 5. System owners communicate with account administrators through a help desk system to identify and document approved users and to grant, review, deactivate, update, and/or terminate account access based upon that communication. 6. Remote access to the system is only permitted through secure, authenticated, and centrally managed access methods (e.g. VPN). 7. System administrators routinely require “privileged” access to the Lenel OnGuard system to perform essential system administration functions. The number of privileged accounts must be kept to a minimum and only provided to those individuals knowledgeable about the IT used in the system and whose job duties require it. 8. Environmental safeguards are used for controlling physical access to equipment and data rooms. Only a limited number of personnel will have physical access to the data center including Information Technology personnel, maintenance personnel, Public Safety and key administrators.

9.2 Granting OnGuard Access

Requirements	Procedures
[R4]	1. For a new hire, Human Resources emails the new user's direct supervisor (cc's Information Technology) relevant employment information along with a link to an electronic access request form. 2. The user's direct supervisor must complete and submit the *Computer Access Form – New Employee* online to initiate account creation and determine what level of access is allowed (i.e. query and/or modify). Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 3. If the direct supervisor has not been identified as a system owner for Lenel OnGuard, the system owner is contacted by the account administrator and approval is substantiated before access is granted. Access privileges should be commensurate with the user's defined responsibilities. 4. The account administrator creates account access in Lenel and synchronizes with the user's domain account after receiving proper approval from the system owner. 5. The user's supervisor receives notification that access has been granted from the account administrator after the account has been created. Note: appropriate permissions assigned to the account – taking into consideration the principle of least privilege and separation of duties – is the responsibility of both the supervisor and the system owner. 6. The supervisor will distribute system information to the new user and verify access. 7. Communication between Human Resources, system owners, supervisors, and account administrators will be documented via the help desk ticketing system.

9.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** 1. Human Resources is notified of an employee's pending termination and/or need for account deactivation. 2. To officially initiate user account deactivation, Human Resources will send the user's direct supervisor (cc's Information Technology) an email with a link to an electronic termination request form. 3. The user's direct supervisor must complete and submit the *Computer Access Form – Employee Terminated Checklist* online. 4. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Within **five (5)** business days* of form submission the account administrator will: • Remove all user privileges • Deactivate the user's account • Document completion and notify employee's supervisor and Human Resources * when an employee is terminated for cause, account deactivation must occur immediately. **Personnel Status Changes** 1. For changes to existing user accounts not within the scope of termination/deactivation, a *Computer Access Form - Change Employee Access* form must be completed by the user's direct supervisor. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 2. If the direct supervisor has not been identified as a system owner for any additional system privileges requested, the system owner is contacted by the account administrator and approval is substantiated before any additional access is granted. Access privileges should be commensurate with the user's defined responsibilities. 3. To maintain the requirements of least privilege, when a user transfers to a new role and/or department, all privileges should first be removed and then new privileges added that are required in the user's new role. 4. Within **thirty (30)** days of user status changes the account administrator will: • Remove user privileges (if applicable) • Update system access • Document changes and notify employee's supervisor

9.4 User Access Review

Requirements	Procedures
[R2] [R4]	1. The account administrator provides the system owner a list of users and associated roles every **four (4)** months. An up-to-date list of users is also available upon request. 2. A user access list is submitted by the account administrator to the system owner for review via the help desk ticketing system. A system owner acknowledges the list has been reviewed by responding to the ticket via email and requests any changes, if applicable. 3. The account administrator modifies user access and the system owner is notified. 4. The account administrator documents the entire transaction in the help desk ticketing system. 5. System owners are assigned a **one (1)** month time frame to complete the user access review. 6. A status report is submitted to the Vice President of Business Affairs following the allotted time frame.

Section 10: Raiser's Edge

Raiser's Edge is an information system developed by Blackbaud, Inc and used primarily for tracking alumni and the college's fundraising efforts.

10.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	1. The institution will protect information resources in Raiser's Edge by adopting and implementing the user access standards set forth in this document. 2. System owners and supervisors will inform all employees about the importance of keeping their access information safe. 3. Account administrator will ensure unique identification of each user and assignment of access privileges. 4. System owners communicate with account administrators through a help desk system to identify and document approved users and to grant, review, deactivate, update, and/or terminate account access based upon that communication. 5. System administrators routinely require "privileged" access to the Raiser's Edge system to perform essential system administration functions. The number of privileged accounts must be kept to a minimum and only provided to those individuals knowledgeable about the IT used in the system and whose job duties require it. 6. Environmental safeguards are used for controlling physical access to equipment and data rooms. Only a limited number of personnel will have physical access to the data center including Information Technology personnel, maintenance personnel, Public Safety and key administrators.

10.2 Granting Raiser's Edge Access

Requirements	Procedures
[R4]	1. For a new hire, Human Resources emails the new user's direct supervisor (cc's Information Technology) relevant employment information along with a link to an electronic access request form. 2. The user's direct supervisor must complete and submit the *Computer Access Form – New Employee* online to initiate account creation and determine what Raiser's Edge roles are required. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 3. If the direct supervisor has not been identified as a system owner for Raiser's Edge, the system owner is contacted by the account administrator and approval is substantiated before access is granted. Access privileges should be commensurate with the user's defined responsibilities. 4. The account administrator creates account access after receiving proper approval from the system owner. 5. The user's supervisor receives account information from the account administrator after the account has been created. Note: appropriate permissions assigned to the account – taking into consideration the principle of least privilege – is the responsibility of both the supervisor and the system owner. 6. The supervisor will distribute account information to the new user and verify the temporary password has been changed. 7. Communication between Human Resources, system owners, supervisors, and account administrators will be documented via the help desk ticketing system.

10.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** 5. Human Resources is notified of an employee's pending termination and/or need for account deactivation. 6. To officially initiate user account deactivation, Human Resources will send the user's direct supervisor (cc's Information Technology) an email with a link to an electronic termination request form. 7. The user's direct supervisor must complete and submit the *Computer Access Form – Employee Terminated Checklist* online. 8. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Within **five (5)** business days* of form submission the account administrator will: • Remove all user privileges • Deactivate the user's account • Document completion and notify employee's supervisor and Human Resources * when an employee is terminated for cause, account deactivation must occur immediately. **Personnel Status Changes** 5. For changes to existing user accounts not within the scope of termination/deactivation, a *Computer Access Form - Change Employee Access* form must be completed by the user's direct supervisor. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 6. If the direct supervisor has not been identified as a system owner for any additional system privileges requested, the system owner is contacted by the account administrator and approval is substantiated before any additional access is granted. Access privileges should be commensurate with the user's defined responsibilities. 7. To maintain the requirements of least privilege, when a user transfers to a new role and/or department, all privileges should first be removed and then new privileges added that are required in the user's new role. 8. Within **thirty (30)** days of user status changes the account administrator will: • Remove user privileges (if applicable) • Update system access • Document changes and notify employee's supervisor

10.4 User Access Review

Requirements	Procedures
[R2] [R4]	1. The account administrator provides the system owner a list of users and associated roles every **four (4)** months. An up-to-date list of users is also available upon request. 2. A user access list is submitted by the account administrator to the system owner for review via the help desk ticketing system. A system owner acknowledges the list has been reviewed by responding to the ticket via email and requests any changes, if applicable. 3. The account administrator modifies user access and the system owner is notified. 4. The account administrator documents the entire transaction in the help desk ticketing system. 5. System owners are assigned a **one (1)** month time frame to complete the user access review. 6. A status report is submitted to the Vice President of Business Affairs following the allotted time frame.

Section 11: DegreeWorks

DegreeWorks, developed by Ellucian (formerly Sungard Higher Education), provides a comprehensive set of web-based academic advising, degree audit, and transfer articulation tools to help students and their advisors negotiate the college's curriculum requirements.

11.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	To authenticate access, DegreeWorks user accounts are configured for single sign-on by synchronizing with a user's Banner Web account. See Section 4.1 under Banner Web for authentication and authorized access mechanisms and processes.

11.2 Granting DegreeWorks Access

Requirements	Procedures
[R4]	**Students** 1. The admissions personnel input student enrollment data into the Banner system. 2. The system uses the information to generate a GCID and create a record in the Banner Web user table. 3. All currently enrolled student accounts are automatically loaded into the DegreeWorks system via shell scripts. Student accounts are synchronized with Banner Web via single sign-on. 4. Student permissions are set automatically according to the principle of least privilege (Student role). 5. Students access the DegreeWorks system through Banner Web. Students are trained on how to login and change access information to Banner Web during orientation sessions. Students also receive an enrollment packet with instructions on how to initiate access. **Faculty/Advisors** 1. See Granting Banner Web Access (3.2) for information on how Banner Web accounts are provisioned for faculty. 2. All full-time active faculty are loaded into the DegreeWorks system via shell scripts. Faculty accounts are synchronized with Banner Web via single sign-on. 3. Faculty permissions are set automatically according to the principle of least privilege (Advisor role). 4. If additional access is required, the employee's direct supervisor should contact the Registrar for approval and role assignment. **User access is managed by the Registrar.** 5. A faculty member receives DegreeWorks information from his or her academic department. The Office of the Registrar also holds regular training sessions on DegreeWorks.

	Staff 1. Only administrative users from the Registrar, Academic Affairs, and selected Information Technology personnel need access to DegreeWorks. **User access is managed by the Registrar.** 2. Any employee access request for DegreeWorks must be communicated to the Registrar by the user's direct supervisor. Access privileges should be commensurate with the user's defined responsibilities. 3. The user's supervisor receives DegreeWorks information from the Registrar after the user account has been setup. 4. The supervisor will distribute this information to the new user. The Office of the Registrar also holds regular training sessions on DegreeWorks.

11.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** Students Student accounts are **never** terminated /deactivated. Student accounts are available to them indefinitely as it has important information concerning past academic records. Faculty/Staff See Terminating, Updating, and/or Deactivating User Access (3.3) for information on how Banner Web accounts are terminated and/or deactivated. **Personnel Status Changes** 1. Updates concerning terminations and personnel status changes are not applicable to student accounts. 2. Most faculty and staff are assigned access at the lowest level of the principle of least privilege therefore; personnel status changes requiring system privilege updates are uncommon. Personnel status changes are reviewed on a case-by-case basis by the Registrar.

11.4 User Access Review

Requirements	Procedures
[R2] [R4]	1. The DegreeWorks system administrator provides the system owner a list of users and associated roles every **four (4)** months (incl. students, advisors, and staff roles). An up-to-date list of users is also available upon request. 2. A user access list is submitted by the system administrator to the system owner for review via the help desk ticketing system. The system owner acknowledges the list has been reviewed by responding to the ticket via email and notifies the system administrator if any changes were made in the system by the Registrar. **User access is managed by the Registrar.** 3. The system administrator documents the entire transaction in the help desk ticketing system. 4. System owners are assigned a **one (1)** month time frame to complete the user access review. 5. A status report is submitted to the Vice President of Business Affairs following the allotted time frame.

Section 12: Crystal Reports

Crystal Reports, developed by SAP, is a business intelligence platform for creating and delivering powerful, interactive reports from any data source over the Web.

12.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	1. Each department will protect information resources in Crystal Reports by adopting and implementing the user access standards set forth in this document. 2. System owners and supervisors will inform prospective users about the importance of keeping their access information safe. 3. Account administrator will ensure unique identification of each user and assignment of access privileges. 4. Users are required to create a specific unique password after they login with the account information provided to them at initial setup, and to create a new password every 180 days. Users can not choose any of their last five (5) previously used passwords. 5. Accounts are locked after 5 unsuccessful logon attempts for duration of five (5) minutes. 6. System owners communicate with account administrators through a help desk system to identify and document approved users and to grant, review, deactivate, update, and/or terminate account access based upon that communication. 7. To prevent and detect unauthorized use, system administrators monitor logs generated by Crystal Reports and other internal systems. Any unusual activity is investigated by Information Technology. Potential threats are handled on a case-by-case basis with respect to risk level. 8. System administrators routinely require “privileged” access to the Crystal Reports system to perform essential system administration functions. The number of privileged accounts must be kept to a minimum and only provided to those individuals knowledgeable about the IT used in the system and whose job duties require it. 9. Environmental safeguards are used for controlling physical access to equipment and data rooms. Only a limited number of personnel will have physical access to the data center including Information Technology personnel, maintenance personnel, Public Safety and key administrators.

12.2 Granting Crystal Reports Access

Requirements	Procedures
[R4]	1. For a new hire, Human Resources emails the new user's direct supervisor (cc's Information Technology) relevant employment information along with a link to an electronic access request form. 2. The user's direct supervisor must complete and submit the *Computer Access Form – New Employee* online to initiate account creation and determine what Crystal Reports roles are required. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 3. The account administrator creates account access after receiving proper approval from the system owner. 4. The user's supervisor receives account information from the account administrator after the account has been created. Note: appropriate permissions assigned to the account – taking into consideration the principle of least privilege – is the responsibility of both the supervisor and the system owner. 5. The supervisor will distribute account information to the new user and verify the temporary password has been changed. 6. Communication between Human Resources, system owners, supervisors, and account administrators will be documented via the help desk ticketing system.

12.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** 1. Human Resources is notified of an employee's pending termination and/or need for account deactivation. 2. To officially initiate user account deactivation, Human Resources will send the user's direct supervisor (cc's Information Technology) an email with a link to an electronic termination request form. 3. The user's direct supervisor must complete and submit the *Computer Access Form – Employee Terminated Checklist* online. 4. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Within **five (5)** business days* of form submission the account administrator will: • Remove all user privileges • Deactivate the user's account • Document completion and notify employee's supervisor and Human Resources * when an employee is terminated for cause, account deactivation must occur immediately.

	Personnel Status Changes 1. For changes to existing user accounts not within the scope of termination/deactivation, a *Computer Access Form - Change Employee Access* form must be completed by the user's direct supervisor. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 2. If the direct supervisor has not been identified as a system owner for any additional system privileges requested, the system owner is contacted by the account administrator and approval is substantiated before any additional access is granted. Access privileges should be commensurate with the user's defined responsibilities. 3. To maintain the requirements of least privilege, when a user transfers to a new role and/or department, all privileges should first be removed and then new privileges added that are required in the user's new role. 4. Within **thirty (30)** days of user status changes the account administrator will: • Remove user privileges (if applicable) • Update system access • Document changes and notify employee's supervisor

12.4 User Access Review

Requirements	Procedures
[R2] [R4]	1. The account administrator provides the system owner a list of users and associated roles every **four (4)** months. An up-to-date list of users is also available upon request. 2. A user access list is submitted by the account administrator to the system owner for review via the help desk ticketing system. A system owner acknowledges the list has been reviewed by responding to the ticket via email and requests any changes, if applicable. 3. The account administrator modifies user access and the system owner is notified. 4. The account administrator documents the entire transaction in the help desk ticketing system. 5. System owners are assigned a **one (1)** month time frame to complete the user access review. 6. A status report is submitted to the Vice President of Business Affairs following the allotted time frame.

Section 13: Touchnet System – Bill+Payment, SponsorPoint, MarketPlace

Bill+Payment is a comprehensive "payment portal" for student accounts.

SponsorPoint is a comprehensive "payment portal" for third party institutional payers.

MarketPlace is a comprehensive framework for eCommerce throughout the campus.

13.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	**Students** To authenticate access, Touchnet Bill Pay user accounts are configured for single sign-on by synchronizing with a user's Banner Web account. See Section 4.1 under Banner Web for authentication and authorized access mechanisms and processes. **Staff** 1. Each department will protect information resources in Touchnet Bill Pay by adopting and implementing the user access standards set forth in this document. 2. System owners and supervisors will inform prospective users about the importance of keeping their access information safe. 3. Internal communications, mitigating controls for segregation of duties, and well-defined workflows are all utilized to verify authorized access and protect resources. 4. Account administrator will ensure unique identification of each user and assignment of access privileges. 5. Users are required to create a specific unique password after initial setup, and to create a new password every 90 days. 6. Accounts are locked after 3 unsuccessful attempts. 7. System owners communicate with account administrators through a help desk system to identify and document approved users and to grant, review, deactivate, update, and/or terminate account access based upon that communication.

13.2 Granting Touchnet Bill Pay Access

Requirements	Procedures
[R4]	**Students** 1. The admissions personnel input student enrollment data into the Banner system. 2. The system uses the information to generate a GCID and create a record in the Banner Web user table. 3. All currently enrolled student accounts are automatically loaded into the Touchnet Bill Pay system via file uploads. Student accounts are synchronized with Banner Web via single sign-on. 4. Student permissions are set automatically according to the principle of least privilege (Student role). 5. Students access the Touchnet Bill Pay system through Banner Web. Students are trained on how to login and change access information to Banner Web during orientation sessions. Students also receive an enrollment packet with instructions on how to initiate access. **Staff** 1. Only users from the Business Office and selected Information Technology personnel need access to Touchnet Bill Pay. **User access is managed by the Director of Business Services.** 2. Any employee access request for Touchnet Bill Pay must come directly from the Director of Business Services. Access privileges should be commensurate with the user's defined responsibilities. 3. The Director of Business Services receives information from Information Technology after the user account has been setup. 4. The supervisor will distribute this information to the new user. The Director of Business Services will provide training for the use of Touchnet Bill Pay. **Third Party Payers (SponsorPoint Only)** Third party payers are sent by email a link to set up an account by the Business Office staff that has Sponsor Point Admin Access. They establish their own account.

13.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** **Students** Student accounts are **never** terminated /deactivated. Student accounts are available to them indefinitely as it has important information concerning past academic records. **Staff** 1. Human Resources is notified of an employee's pending termination and/or need for account deactivation. 2. To officially initiate user account deactivation, Human Resources will send the user's direct supervisor (cc's Information Technology) an email with a link to an electronic termination request form. 3. The user's direct supervisor must complete and submit the *Computer Access Form – Employee Terminated Checklist* online. 4. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Within **five (5)** business days* of form submission the account administrator will: • Remove all user privileges • Deactivate the user's account • Document completion and notify employee's supervisor and Human Resources * when an employee is terminated for cause, account deactivation must occur immediately. **Third Party Payers (SponsorPoint Only)** Accounts for Third party payers who no longer have business with the college are deactivated by the Business Office Staff that has SponsorPoint Admin Access. **Personnel Status Changes** 1. For changes to existing user accounts not within the scope of termination/deactivation, a *Computer Access Form - Change Employee Access* form must be completed by the user's direct supervisor. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 2. To maintain the requirements of least privilege, when a user transfers to a new role and/or department, all roles should first be removed and then new roles added that are required in the user's new position. 3. Within **thirty (30)** days of user status changes the account administrator will: • Remove user roles (if applicable) • Update system access Document changes and notify employee's supervisor

13.4 User Access Review

Requirements	Procedures
[R2] [R4]	1. The Touchnet Bill Pay system administrator provides the system owner a list of users and associated roles every **four (4)** months. An up-to-date list of users is also available upon request. 2. A user access list is submitted by the system administrator to the system owner for review via the help desk ticketing system. The system owner acknowledges the list has been reviewed by responding to the ticket via email and notifies the system administrator if any changes were made in the system by the Director of Business Services. **User access is managed by the Director of Business Services.** 3. The system administrator documents the entire transaction in the help desk ticketing system. 4. System owners are assigned a **one (1)** month time frame to complete the user access review. 5. A status report is submitted to the Vice President of Business Affairs following the allotted time frame.

Section 14: Touchnet PayPath System

Touchnet Paypath is software used in conjunction with Touchnet Bill Payment to process credit card payments for student accounts.

14.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	1. Each department will protect information resources in Touchnet PayPath by adopting and implementing the user access standards set forth in this document. 2. System owners and supervisors will inform prospective users about the importance of keeping their access information safe. 3. Account administrator will ensure unique identification of each user and assignment of access privileges. 4. Users are required to create a specific unique password after initial setup, and to create a new password every 90 days. 5. Accounts are locked after 3 unsuccessful attempts. 6. System owners communicate with account administrators through a help desk system to identify and document approved users and to grant, review, deactivate, update, and/or terminate account access based upon that communication.

14.2 Granting Touchnet PayPath Access

Requirements	Procedures
[R4]	1. Only users from the Business Office and selected Information Technology personnel require access to Touchnet PayPath. **User access is managed by the Director of Business Services and Touchnet.** 2. Authorization for employee access to Touchnet Bill PayPath must come directly from the Director of Business Services. Touchnet handles all account provisioning. 3. The Director of Business Services will open a ticket with Touchnet requesting a new PayPath user account. Any access privileges granted should be commensurate with the user's defined responsibilities. 4. The Director of Business Services receives information from Touchnet after the user account has been setup. 5. The supervisor will distribute this information to the new user. The Director of Business Services will provide training for the use of Touchnet PayPath.

14.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** 1. Human Resources is notified of an employee's pending termination and/or need for account deactivation. 2. To officially initiate user account deactivation, Human Resources will send the user's direct supervisor an email – *in most all cases the Director of Business Services* (cc's Information Technology) – with a link to an electronic termination request form. 3. The user's direct supervisor must complete and submit the *Computer Access Form – Employee Terminated Checklist* online. 4. If user has a Paypath account, the Director of Business Services will contact Touchnet and request account deactivation within five (5) business days of employee separation * * when an employee is terminated for cause, account deactivation must occur immediately. **Personnel Status Changes** 1. For changes to existing user accounts not within the scope of termination/deactivation, the Director of Business Services will be notified immediately. 2. The Director of Business Services will contact Touchnet and request an update to system access. Personnel status changes are reviewed on a case-by-case basis by the Director of Business Services.

14.4 User Access Review

Requirements	Procedures
[R2] [R4]	1. The Touchnet PayPath system administrator provides the system owner a list of users and associated roles every **four (4)** months. An up-to-date list of users is also available upon request. 2. A user access list is submitted by the system administrator to the system owner for review via the help desk ticketing system. The system owner acknowledges the list has been reviewed by responding to the ticket via email and notifies the system administrator if any changes were made in the system by the Director of Business Services. **User access is managed by the Director of Business Services.** 3. The system administrator documents the entire transaction in the help desk ticketing system. 4. System owners are assigned a **one (1)** month time frame to complete the user access review. 5. A status report is submitted to the Vice President of Business Affairs following the allotted time frame.

Section 15: Commvault Simpana

Commvault Simpana software is an enterprise level backup and disaster recovery solution.

15.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	1. System administrators routinely require “privileged” access to the Commvault system to perform essential system administration functions. The number of users with access to Commvault must be kept to a minimum and only provided to those individuals knowledgeable about the IT used in the system and whose job duties require it. 2. The Director of Information Technology uses internal communication to identify approved users and to grant, review, deactivate, update, and/or terminate account access. 3. To authenticate access, a Commvault user account is configured for single sign-on by synchronizing with a Domain account. The same user access controls for Domain accounts apply (see section 8). 4. To prevent and detect unauthorized use, the system administrator monitors logs generated by Commvault and other internal systems. Any unusual activity is investigated by Information Technology. Potential threats are handled on a case-by-case basis with respect to risk level. 5. Remote access to the system is only permitted through secure, authenticated, and centrally managed access methods (e.g. VPN). 6. Environmental safeguards are used for controlling physical access to equipment and data rooms. Only a limited number of personnel will have physical access to the data center including Information Technology personnel, maintenance personnel, Public Safety and key administrators.

15.2 Granting Commvault Simpana Access

Requirements	Procedures
[R4]	1. The Director of Information Technology verifies access to the Commvault system is appropriate for an employee's defined job responsibilities. 2. The system administrator receives an official request from the Director of Information Technology on behalf of an employee needing access to the Commvault system. 3. After receiving the request for access from the Director, the System Administrator will verify the user's existing Domain account and will add the account to the appropriate Active Directory group synchronized with the Commvault system. **Note:** The principle of least privilege is not applicable to the Commvault account provisioning process. All users have the same privilege level.

15.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** 1. The system administrator receives notification from the Director of Information Technology identifying the user whose access to Commvault should be revoked. 2. Immediately upon notification the system administrator will: • Change shared "privileged" account password • Remove user from the Commvault Active Directory group • Verify that the Domain account has been deactivated (see section 8.3) • Document via the help desk ticketing system. **Personnel Status Changes** Immediately upon notification of a personnel status change the system administrator will: • Change shared "privileged" account password. • Remove user privileges to Commvault system (if applicable) • Document via the help desk ticketing system.

15.4 User Access Review

Requirements	Procedures
[R2] [R4]	1. The system administrator reviews Commvault accounts every **four (4)** months. 2. The system administrator will discuss needed modifications with the Director of Information Technology. The modifications can be made upon the Director's request. 3. The system administrator documents the process in the help desk ticketing system.

Section 16: PaloAlto Firewall

A next-generation firewall from PaloAlto (PA) networks that is used by the college to protect and manage the college network infrastructure.

16.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	1. IT uses a single shared administrator account to manage the PaloAlto Firewall to perform essential system administration functions. The number of users with access to the PaloAlto Firewall must be kept to a minimum and only provided to those individuals knowledgeable about the IT used in the system and whose job duties require it. 2. The Director of Information Technology uses internal communication to identify approved users and manage account access. 3. To prevent and detect unauthorized use, the system administrator monitors logs generated by the PA and other internal systems. Any unusual activity is investigated by Information Technology. Potential threats are handled on a case-by-case basis with respect to risk level. 4. Remote access to the system is only permitted through secure, authenticated, and centrally managed access methods (e.g. VPN). 5. Environmental safeguards are used for controlling physical access to equipment and data rooms. Only a limited number of personnel will have physical access to the data center including Information Technology personnel, maintenance personnel, Public Safety and key administrators.

16.2 Granting PaloAlto Firewall Access

Requirements	Procedures
[R4]	1. The Director of Information Technology verifies access to the PA system is appropriate for an employee's defined job responsibilities. 2. The Director of Information Technology provides the employee the shared account credentials. **Note:** The principle of least privilege is not applicable to the PA system. A single shared account is managed internally within the IT Office.

16.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** 1. The Director of Information Technology identifies the user whose access to the PaloAlto Firewall should be revoked. 2. Immediately upon notification a system administrator or Director of Information Technology will: • Change shared account password • Document via the help desk ticketing system. **Personnel Status Changes** Immediately upon notification of a personnel status change the system administrator or Director of Information Technology will: • Change shared account password if access is no longer required as part of the employee's newly assigned job responsibilities. • Document via the help desk ticketing system.

16.4 User Access Review

Requirements	Procedures
[R2] [R4]	1. The Director of Information Technology reviews PaloAlto Firewall account access every **four (4)** months. 2. The Director of Information Technology documents the process in the help desk ticketing system.

Section 17: Equallogic SAN

The Equallogic is a storage area network (SAN) developed by Dell and is used by the college for consolidated drive storage in a virtualized environment.

17.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	1. IT uses a single shared administrator account to manage the Equallogic SAN to perform essential system administration functions. The number of users with access to the SAN must be kept to a minimum and only provided to those individuals knowledgeable about the IT used in the system and whose job duties require it. 2. The Director of Information Technology uses internal communication to identify approved users and manages account access. 3. To prevent and detect unauthorized use, the system administrator monitors logs generated by the SAN and other internal systems. Any unusual activity is investigated by Information Technology. Potential threats are handled on a case-by-case basis with respect to risk level. 4. Remote access to the system is only permitted through secure, authenticated, and centrally managed access methods (e.g. VPN). 5. Environmental safeguards are used for controlling physical access to equipment and data rooms. Only a limited number of personnel will have physical access to the data center including Information Technology personnel, maintenance personnel, Public Safety and key administrators.

17.2 Granting Equallogic SAN Access

Requirements	Procedures
[R4]	1. The Director of Information Technology verifies access to the Equallogic SAN is appropriate for an employee's defined job responsibilities. 2. The Director of Information Technology provides the employee the shared account credentials. **Note:** The principle of least privilege is not applicable to the SAN. A single shared account is managed internally within the IT Office.

17.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** 1. The Director of Information Technology identifies the user whose access to the Equallogic SAN should be revoked. 2. Immediately upon notification a system administrator or Director of Information Technology will: • Change shared account password • Document via the help desk ticketing system. **Personnel Status Changes** Immediately upon notification of a personnel status change the system administrator or Director of Information Technology will: • Change shared account password if access is no longer required as part of the employee's newly assigned job responsibilities. • Document via the help desk ticketing system.

17.4 User Access Review

Requirements	Procedures
[R2] [R4]	1. The Director of Information Technology reviews Equallogic SAN account access every **four (4)** months. 2. The Director of Information Technology documents the process in the help desk ticketing system.

Section 18: DHCP

Dynamic Host Configuration Protocol (DHCP) is a network protocol used for dynamically distributing network configurations to hosts within IP networks.

18.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	1. System administrators routinely require "privileged" account access to DHCP services to perform essential system administration functions. The number of users with access to DHCP must be kept to a minimum and only provided to those individuals knowledgeable about the IT used in the system and whose job duties require it. 2. The Director of Information Technology uses internal communication to identify approved users and to grant, review, deactivate, update, and/or terminate account access. 3. To authenticate access, only members of the Domain Admins group can administer DHCP. The same user access controls for Domain accounts apply (see section 8). 4. To prevent and detect unauthorized use, firewall policies are applied and the system administrator monitors logs generated by network/firewall systems. Any unusual activity is investigated by Information Technology. Potential threats are handled on a case-by-case basis with respect to risk level. 5. Remote access to the system is only permitted through secure, authenticated, and centrally managed access methods (e.g. VPN). 6. Environmental safeguards are used for controlling physical access to equipment and data rooms. Only a limited number of personnel will have physical access to the data center including Information Technology personnel, maintenance personnel, Public Safety and key administrators.

18.2 Granting DHCP Access

Requirements	Procedures
[R4]	1. The Director of Information Technology verifies access to DHCP services is appropriate for an employee's defined job responsibilities. 2. The system administrator receives an official request from the Director of Information Technology on behalf of an employee needing access to DHCP services. 3. After receiving the request for access from the Director, the System Administrator will verify the user's existing Domain account and will add the account to the appropriate Active Directory group. **Note:** The principle of least privilege is not applicable to the DHCP account provisioning process. All users have the same privilege level.

18.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** 1. The system administrator receives notification from the Director of Information Technology identifying the user whose access to DHCP should be revoked. 2. Immediately upon notification the system administrator will: • Change shared "privileged" account password • Remove user from the appropriate Active Directory groups • Verify that the Domain account has been deactivated (see section 8.3) • Document via the help desk ticketing system. **Personnel Status Changes** Immediately upon notification of a personnel status change the system administrator will: • Change shared "privileged" account password. • Remove user from the appropriate Active Directory groups • Document via the help desk ticketing system.

18.4 User Access Review

Requirements	Procedures
[R2] [R4]	1. The system administrator reviews DHCP access every **four (4)** months. 2. The system administrator will discuss needed modifications with the Director of Information Technology. The modifications can be made upon the Director's request. 3. The system administrator documents the process in the help desk ticketing system.

Section 19: DNS

Domain Name Services (DNS) is a naming system for networks that translate human-readable names to IP addresses.

19.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	1. System administrators routinely require "privileged" account access to DNS services to perform essential system administration functions. The number of users with access to DNS must be kept to a minimum and only provided to those individuals knowledgeable about the IT used in the system and whose job duties require it. 2. The Director of Information Technology uses internal communication to identify approved users and to grant, review, deactivate, update, and/or terminate account access. 3. To authenticate access, only members of the Domain Admins group can administer DNS. The same user access controls for Domain accounts apply. 4. To prevent and detect unauthorized use, firewall policies are applied and the system administrator monitors logs generated by network/firewall systems. Any unusual activity is investigated by Information Technology. Potential threats are handled on a case-by-case basis with respect to risk level. 5. Remote access to the system is only permitted through secure, authenticated, and centrally managed access methods (e.g. VPN). 6. Environmental safeguards are used for controlling physical access to equipment and data rooms. Only a limited number of personnel will have physical access to the data center including Information Technology personnel, maintenance personnel, Public Safety and key administrators.

19.2 Granting DNS Access

Requirements	Procedures
[R4]	1. The Director of Information Technology verifies access to DNS is appropriate for an employee's defined job responsibilities. 2. The system administrator receives an official request from the Director of Information Technology on behalf of an employee needing access to DNS services. 3. After receiving the request for access from the Director, the System Administrator will verify the user's existing Domain account and will add the account to the appropriate Active Directory group. **Note:** The principle of least privilege is not applicable to the DNS account provisioning process. All users have the same privilege level.

19.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** 1. The system administrator receives notification from the Director of Information Technology identifying the user whose access to DNS should be revoked. 2. Immediately upon notification the system administrator will: • Change shared "privileged" account password • Remove user from the appropriate Active Directory groups • Verify that the Domain account has been deactivated (see section 8.3) • Document via the help desk ticketing system. **Personnel Status Changes** Immediately upon notification of a personnel status change the system administrator will: • Change shared "privileged" account password. • Remove user from the appropriate Active Directory groups • Document via the help desk ticketing system.

19.4 User Access Review

Requirements	Procedures
[R2] [R4]	1. The system administrator reviews DNS access every **four (4)** months. 2. The system administrator will discuss needed modifications with the Director of Information Technology. The modifications can be made upon the Director's request. 3. The system administrator documents the process in the help desk ticketing system.

Section 20: TutorTrac

TutorTrac is online management software developed by Redrock Software and used by the college's Student Success Center to track registrations in courses, record visits to the center, and report on student progress.

20.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	1. The Student Success Center will protect information resources in TutorTrac by adopting and implementing the user access standards set forth in this document. 2. System owners and supervisors will inform prospective users about the importance of keeping their access information safe. 3. Account administrator will ensure unique identification of each user and assignment of access privileges. 4. System administrators routinely require "privileged" account access to TutorTrac to perform essential system administration functions. The number of users with access to the TutorTrac system account must be kept to a minimum and only provided to those individuals knowledgeable about the application and whose job duties require it. 5. To prevent unauthorized access accounts must be requested by the Director of Student Success on behalf of the employee requesting access. Only individuals from the Student Success Center need access to TutorTrac. 6. To prevent and detect unauthorized use, firewall policies are applied and the system administrator monitors logs generated by network/firewall systems. Any unusual activity is investigated by Information Technology. Potential threats are handled on a case-by-case basis with respect to risk level. 7. Remote access to the system is only permitted through secure, authenticated, and centrally managed access methods (e.g. VPN). 8. Environmental safeguards are used for controlling physical access to equipment and data rooms. Only a limited number of personnel will have physical access to the data center including Information Technology personnel, maintenance personnel, Public Safety and key administrators.

20.2 Granting TutorTrac Access

Requirements	Procedures
[R4]	1. The account administrator receives a user access notification request directly from the Director of Student Success. 2. The Director of Student Success works with the account administrator to determine appropriate access privileges based on the user's defined responsibilities. Note: appropriate permissions assigned to the account – taking into consideration the principle of least privilege – is the responsibility of the Director of Student Success. 3. The account administrator creates account access in TutorTrac. 4. The Director of Student Success receives notification that access has been granted from the account administrator after the account has been created. 5. The supervisor will distribute system information to the new user and verify access. 6. Communications between account administrator and Director of Student Success will be documented via the help desk ticketing system.

20.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** 1. To initiate deactivation, the account administrator receives notification from the Directory of Student Success. 2. Within **five (5)** business days* of form submission the account administrator will: • Remove all user privileges • Deactivate the user's account • Document completion and notify the Directory of Student Success * when an employee is terminated for cause, account deactivation must occur immediately. **Personnel Status Changes** 1. Personnel status changes are received from the Director of Student Success and accounts are adjusted per section 20.2. 2. To maintain the requirements of least privilege, when a user transfers to a new role and/or department, all privileges should first be removed and then new privileges added that are required in the user's new role. 3. Within **thirty (30)** days of user status changes the account administrator will: • Remove user privileges (if applicable) • Update system access • Document changes and notify Director of Student Success

20.4 User Access Review

Requirements	Procedures
[R2] [R4]	1. The account administrator provides the Director of Student Success with a list of users that have access to TutorTrac every **four (4)** months. An up-to-date list of users is also available upon request. 2. A user access list is submitted by the account administrator to the Director of Student Success for review via the help desk ticketing system. A system owner acknowledges the list has been reviewed by responding to the ticket via email and requests any changes, if applicable. 3. The account administrator modifies user access and the Director of Student Success is notified. 4. The account administrator documents the entire transaction in the help desk ticketing system. 5. System owners are assigned a **one (1)** month time frame to complete the user access review. 6. A status report is submitted to the Vice President of Business Affairs following the allotted time frame.

Section 21: SQL Server

21.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	1. System administrators routinely require "privileged" access to the SQL Server database to perform essential system administration functions. The number of privileged accounts must be kept to a minimum and only provided to those individuals knowledgeable about the IT used in the system and whose job duties require it. 2. The database administrator uses internal communication to identify approved users and maintains shared account credentials. 3. Additional procedures for granting, reviewing, deactivating, updating, and/or terminating account access should be followed for all front-end client/server applications that use the SQL Server database 4. To prevent and detect unauthorized use, the database and network administrators monitor logs generated by SQL Server and other internal systems. Any unusual activity is investigated by Information Technology. Potential threats are handled on a case-by-case basis with respect to risk level. 5. Remote access to the system is only permitted through secure, authenticated, and centrally managed access methods (e.g. VPN). 6. Environmental safeguards are used for controlling physical access to equipment and data rooms. Only a limited number of personnel will have physical access to the data center including Information Technology personnel, maintenance personnel, Public Safety and key administrators.

21.2 Granting SQL Server Access

Requirements	Procedures
[R4]	**Administrative Accounts** 1. The database administrator receives an official request from the Director of Information Technology on behalf of an employee requesting access to SQL Server administrative account(s). 2. Database administrator verifies access privileges requested are commensurate with the prospective user's defined responsibilities. 3. The database administrator will distribute account information to the new user and inform the user that the account should only be used for essential system administration functions. **Applications** Many hosted applications use SQL Server for the backend database which requires provisioning of accounts/roles to access the data. These applications usually create the SQL Server roles and users during setup within that specific application. If possible, all account provisioning and role assignment should be conducted within

	the front-end application and guidelines for those specific applications should be followed.

21.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** Administrative Accounts 1. The database administrator receives notification from the Director of Information Technology identifying the user whose access to SQL Server accounts should be revoked. 2. Immediately upon notification the database administrator will: • Remove user privileges (if applicable) • Change shared passwords • Document via the help desk ticketing system. Applications If possible, account termination/deactivation should be conducted within the front-end application and guidelines for those specific applications should be followed. **Personnel Status Changes** Administrative Accounts Immediately upon notification of a personnel status change the database administrator will: • Remove user privileges (if applicable) • Change shared passwords • Document via the help desk ticketing system. Applications If possible, personnel status changes should be handled within the front-end application and guidelines for those specific applications should be followed.

21.4 User Access Review

Requirements	Procedures
[R2] [R4]	1. The database administrator provides the Director of Information Technology a list of users that have access to the SQL Server database every **four (4)** months. An up-to-date list of users is also available upon request. 2. A user access list is submitted by the database administrator to the Director of Information Technology for review via the help desk ticketing system. The IT Director acknowledges the list has been reviewed by responding to the ticket via email and requests any changes, if applicable. 3. The database administrator modifies user access and the Director of Information Technology is notified. 4. The database administrator/Director of Information Technology documents the entire transaction in the help desk ticketing system. 5. All system owners are assigned a **one (1)** month time frame to complete the user access review. 6. A status report is submitted to the Vice President of Business Affairs following the allotted time frame.

Section 22: Exchange

Gordon State College email system.

22.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	1. Each department will protect information resources on the Gordon State College network by adopting and implementing the user access standards set forth in this document. 2. System owners and supervisors will inform prospective users about the importance of keeping their access information safe. 3. To authenticate access, email accounts are integrated directly with a Domain account. The same user access controls for Domain accounts apply. 4. System owners communicate with account administrators through a help desk system to identify and document approved users and to grant, review, deactivate, update, and/or terminate account access based upon that communication. 5. To prevent and detect unauthorized use, system administrators monitor network and server logs regularly. Unusual activity is investigated by Information Technology. Potential threats are handled on a case-by-case basis with respect to risk level. 6. System administrators routinely require “privileged” access to the email system to perform essential system administration functions. The number of privileged accounts must be kept to a minimum and only provided to those individuals knowledgeable about the IT used in the system and whose job duties require it. 7. Environmental safeguards are used for controlling physical access to equipment and data rooms. Only a limited number of personnel will have physical access to the data center including Information Technology personnel, maintenance personnel, Public Safety and key administrators.

22.2 Granting Exchange Access

Requirements	Procedures
[R4]	**General Email Access** 1. For a new staff hire, Human Resources personnel emails the new user's direct supervisor (cc's Information Technology) relevant employment information along with a link to an electronic access request form. 2. The user's direct supervisor must complete and submit the *Computer Access Form – New Employee* online to initiate domain/email account creation. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 3. For a new faculty hire, Academic Affairs personnel submits the *Computer Access Form – New Faculty Computer Access* online to initiate domain/email account creation. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 4. The account administrator creates domain account access. E-mail accounts are provisioned at the same time and are associated with a user's domain account. **Note:** The principle of least privilege is not applicable to the e-mail provisioning process. All users have the same privilege level. 5. The user's supervisor or administrative assistant receives account information from the account administrator after the account has been created. 6. The supervisor or administrative assistant will distribute account information to the new user and verify the temporary password has been changed by the user. 7. All communication between Human Resources, Academic Affairs, supervisors, and account administrators will be documented via the help desk ticketing system. **Exchange Administrator Access** 1. The Director of Information Technology verifies system admin access to Exchange is appropriate for an employee's defined job responsibilities. 2. The system administrator receives an official request from the Director of Information Technology on behalf of an employee needing system admin access to Exchange. 3. After receiving the request for access from the Director, the System Administrator will verify the user's existing Domain account and will add the account to the appropriate Active Directory group.

22.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** 1. Human Resources is notified of an employee's pending termination and/or need for account deactivation. 2. To officially initiate user account deactivation, Human Resources will send the user's direct supervisor (cc's Information Technology) an email with a link to an electronic termination request form. 3. The user's direct supervisor must complete and submit the *Computer Access Form – Employee Terminated Checklist* online. Supervisors are encouraged to submit forms at least **three (3)** business days prior to the date of separation. 4. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Within **five (5)** business days* of form submission the account administrator will: • Remove user from all AD groups • Deactivate the user's account • Document completion and notify employee's supervisor and Human Resources 5. The system administrator will purge all deactivated domain and e-mail accounts on a quarterly basis. Email accounts are automatically retained for a 14 day period by the system following deletion. * when an employee is terminated for cause, domain account deactivation must occur immediately. **Personnel Status Changes** 1. Typically, personnel changes do not prompt administrative action because there are no privilege levels specifically for email accounts. 2. Retirees maintain domain/e-mail access. Account administrator will remove all AD group membership following separation.

22.4 User Access Review

Requirements	Procedures
[R2] [R4]	1. See Domain Access Procedures for general email access reviews. 2. Exchange administrator(s) will provide the Director of Information Technology a list of users that have system-level access to Exchange every **four (4)** months. 3. The help desk ticketing system is used to document communication between the Exchange administrator and Director of Information Technology. 4. All system owners are assigned a one (1) month time frame to complete the user access review. 5. A status report is submitted to the Vice President of Business Affairs following the allotted time frame.

Section 23: ReportExec

ReportExec is a complete incident reporting software suite, developed by Competitive Edge Software, and used by the college's Public Safety department.

23.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	1. Each department will protect information resources on the Gordon State College network by adopting and implementing the user access standards set forth in this document. 2. All procedural access controls related to the ReportExec system are managed internally by the Public Safety department. Only individuals from the Public Safety department need access to ReportExec. User access is easily monitored. 3. The Director of Public Safety will inform prospective users about the importance of keeping their access information safe. 4. The Director of Public Safety will ensure unique identification of each user and assignment of access privileges. 5. Public Safety will internally identify and document approved users and grant, review, deactivate, update, and/or terminate account access. 6. To prevent and detect unauthorized use, system administrators monitor network and server logs regularly. Unusual activity is investigated by Information Technology. Public Safety will also periodically monitor logs available within the ReportExec system. Potential threats are handled on a case-by-case basis with respect to risk level. 7. System administrators routinely require "privileged" access to the ReportExec system to perform essential system administration functions. The number of privileged accounts must be kept to a minimum and only provided to those individuals knowledgeable about the IT used in the system and whose job duties require it. 8. Environmental safeguards are used for controlling physical access to equipment and data rooms. Only a limited number of personnel will have physical access to the data center including Information Technology personnel, maintenance personnel, Public Safety and key administrators.

23.2 Granting ReportExec Access

Requirements	Procedures
[R4]	1. The Director of Public Safety manages all user access within the ReportExec system and determines the appropriate level of access required to perform a specific job function – taking into consideration the principle of least privilege. 2. The Director of Public Safety creates account access in ReportExec and assigns access privileges. 3. The Director of Public Safety will distribute system information to the new user and verify access.

23.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** 1. The Director of Public Safety identifies the user whose access to ReportExec should be revoked following a separation. Only individuals from the Public Safety department have access to ReportExec. 2. Immediately upon an employee separation the Director of Public Safety will: • Remove user privileges • Change any shared passwords • Document the transaction **Personnel Status Changes** Immediately upon a personnel status change the Director of Public Safety will: • Add/Remove user privileges • Change shared passwords (if applicable) • Document the transaction

23.4 User Access Review

Requirements	Procedures
[R2] [R4]	1. The Director of Public Safety will review and provide a list of users and associated roles every **four (4)** months to the Information Technology Department. 2. The Director of Public Safety acknowledges the list has been reviewed by responding to a helpdesk ticket via email. The Director of Public Safety will document any changes that were made in the ReportExec system. **User access is managed internally by the Public Safety department.** 3. All system owners are assigned a **one (1)** month time frame to complete the user access review. 4. A status report is submitted to the Vice President of Business Affairs following the allotted time frame.

Section 24: Titanium Scheduler

Titanium Scheduler is an electronic records system used by the college's Counseling Services department.

24.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	1. Each department will protect information resources on the Gordon State College network by adopting and implementing the user access standards set forth in this document. 2. All procedural access controls related to the Titanium Scheduler system are managed internally by the Counseling Services department. Only individuals from the Counseling Services department need access to Titanium Scheduler. User access is easily monitored. 3. The Director of Counseling Services will inform prospective users about the importance of keeping their access information safe. 4. The Director of Counseling Services will ensure unique identification of each user and assignment of access privileges. 5. Counseling Services will internally identify and document approved users and grant, review, deactivate, update, and/or terminate account access. 6. To prevent and detect unauthorized use, system administrators monitor network and server logs regularly. Unusual activity is investigated by Information Technology. Counseling Services will also periodically monitor logs available within the Titanium Scheduler system. Potential threats are handled on a case-by-case basis with respect to risk level. 7. System administrators require "privileged" access to the Titanium Scheduler system to perform essential system administration functions. The number of privileged accounts must be kept to a minimum and only provided to those individuals knowledgeable about the IT used in the system and whose job duties require it. 8. Environmental safeguards are used for controlling physical access to equipment and data rooms. Only a limited number of personnel will have physical access to the data center including Information Technology personnel, maintenance personnel, Public Safety and key administrators.

24.2 Granting Titanium Scheduler Access

Requirements	Procedures
[R4]	1. The Director of Counseling Services manages all user access within the Titanium Scheduler system and determines the appropriate level of access required to perform a specific job function – taking into consideration the principle of least privilege. 2. The Director of Counseling Services creates account access in Titanium Scheduler and assigns access privileges. 3. The Director of Counseling Services will distribute system information to the new user and verify access.

24.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** 1. The Director of Counseling Services identifies the user whose access to Titanium Scheduler should be revoked following a separation. Only individuals from the Counseling Services department have access to Titanium Scheduler. 2. Immediately upon an employee separation the Director of Counseling Services will: • Remove user privileges • Change any shared passwords • Document the transaction **Personnel Status Changes** Immediately upon a personnel status change the Director of Counseling Services will: • Add/Remove user privileges • Change shared passwords (if applicable) • Document the transaction

24.4 User Access Review

Requirements	Procedures
[R2] [R4]	1. The Director of Counseling Services will review and provide a list of users and associated roles every **four (4)** months to the Information Technology Department. 2. The Director of Counseling Services acknowledges the list has been reviewed by responding to a helpdesk ticket via email. The Director of Counseling Services will document any changes that were made in the Titanium Scheduler system. **User access is managed internally by the Counseling Services department.** 3. All system owners are assigned a **one (1)** month time frame to complete the user access review. 4. A status report is submitted to the Vice President of Business Affairs following the allotted time frame.

Section 25: ExpressionEngine (Web Content Management System)

ExpressionEngine is software used by the college to manage the primary website content.

25.1 Authenticate and Verify Authorized Access

Requirements	Procedures
[R3] [R5]	1. Each department will protect information resources in ExpressionEngine by adopting and implementing the user access standards set forth in this document. 2. System owners and supervisors will inform prospective users about the importance of keeping their access information safe. 3. Account administrator will ensure unique identification of each user and assignment of access privileges. 4. Users are required to create a specific unique password after they login with the account information provided to them at initial setup, and should create a new password every 180 days. 5. Accounts are locked after 4 unsuccessful attempts in one minute. 6. System owners communicate with account administrators through a help desk system to identify and document approved users and to grant, review, deactivate, update, and/or terminate account access based upon that communication. 7. To prevent and detect unauthorized use, system administrators monitor network and server logs regularly. Unusual activity is investigated by Information Technology. Account administrators monitor logs generated by the ExpressionEngine system. Potential threats are handled on a case-by-case basis with respect to risk level. 8. System administrators routinely require “privileged” access to the ExpressionEngine system to perform essential system administration functions. The number of privileged accounts must be kept to a minimum and only provided to those individuals knowledgeable about the IT used in the system and whose job duties require it. 9. Environmental safeguards are used for controlling physical access to equipment and data rooms. Only a limited number of personnel will have physical access to the data center including Information Technology personnel, maintenance personnel, Public Safety and key administrators.

25.2 Granting ExpressionEngine Access

Requirements	Procedures
[R4]	1. For a new hire, Human Resources emails the new user's direct supervisor (cc's Information Technology) relevant employment information along with a link to an electronic access request form. 2. The user's direct supervisor must complete and submit the *Computer Access Form – New Employee* online to initiate account creation in ExpressionEngine. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 3. The account administrator will work with the user's direct supervisor to determine the appropriate level of access commensurate with the user's defined responsibilities. 4. The account administrator creates account access following communications with the employee's supervisor. 5. The user's supervisor receives account information from the account administrator after the account has been created. Note: appropriate permissions assigned to the account – taking into consideration the principle of least privilege – is the responsibility of the supervisor. 6. The supervisor will distribute account information to the new user and verify the temporary password has been changed. 7. Communication between Human Resources, system owners, supervisors, and account administrators will be documented via the help desk ticketing system.

25.3 Terminating, Updating, and/or Deactivating User Access

Requirements	Procedures
[R4] [R6] [R7]	**Terminating/Deactivating User Access** 1. Human Resources is notified of an employee's pending termination and/or need for account deactivation. 2. To officially initiate user account deactivation, Human Resources will send the user's direct supervisor (cc's Information Technology) an email with a link to an electronic termination request form. 3. The user's direct supervisor must complete and submit the *Computer Access Form – Employee Terminated Checklist* online. Supervisors are encouraged to submit forms at least **three (3)** business days prior to the date of separation. 4. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Within **five (5)** business days* of form submission the account administrator will: • Deactivate the user's account (assign to banned group) • Document completion and notify employee's supervisor and Human Resources * when an employee is terminated for cause, ExpressionEngine account deactivation must occur immediately.

	Personnel Status Changes 1. For changes to existing ExpressionEngine accounts not within the scope of termination/deactivation, a *Computer Access Form - Change Employee Access* form must be completed by the user's direct supervisor. Form submissions are sent directly to the helpdesk system and are reviewed by the account administrator(s). Requests by phone or email are not acceptable. 2. To maintain the requirements of least privilege, when a user transfers to a new role and/or department, all ExpressionEngine membership should first be removed and then new group privileges assigned that are required in the user's new role. 3. Within **thirty (30)** days of user status changes the account administrator will: • Remove group membership (if applicable) • Update group membership access • Document changes and notify employee's supervisor

25.4 User Access Review

Requirements	Procedures
[R2] [R4]	5. Account administrator provides supervisors and/or department heads a list of ExpressionEngine users under their department every **four (4)** months. 6. The help desk ticketing system is used to document communication between the account administrator and supervisors/department heads. 7. Supervisors/Department heads are assigned a **one (1)** month time frame to complete the domain user review. 8. A status report is submitted to the Vice President of Business Affairs following the allotted time frame. 9. To complement the four month reviews the account administrator audits ExpressionEngine accounts at random to ensure access is appropriate.