Fayetteville Technical Community College

Ellucian System Usage

Ownership Roles and Responsibilities

April 2013

Table of Contents

Preface

The purpose of this document is to define how FTCC governs the use of IT assets that are associated with the Ellucian Colleague System. Colleague is the system used by the college to satisfy all student records and business processing requirements. IT Governance specific to Network, Email, and desktop assets are not discussed in this document.

Governance over the use of college owned IT assets is required to insure efficient, responsible and secure use of technology in a way that is consistent with the college's strategies and objectives, and is the responsibility of every department that utilizes college IT resources. IT Governance defines the roles and responsibilities for the handling and use of information, business processes, applications, and systems, and is the basis for IT Standards followed by the college. This is the focus of much of this document.

In May 2011, all NC community colleges were directed (see CC11-009 in appendix) to begin comparing local IT standards and controls to those standards published in the NC Statewide Information Security Manual, as it has been adopted by the Office of the State Auditor as the basis for all IT Audits. The NC Community College system office is in the process finalizing a new set of standards for the colleges that meets or exceeds those published in the statewide manual. The directive also indicated that according to G.S. § 147-33.111(b), Community Colleges may develop their own standards, provided they are "comparable to or exceed" those published in the "Statewide Security Information manual". As a result of that memo, this document has been updated to be more consistent with the standards published in the NC Statewide Information Security Manual.

Chapters 1, 2 and 11 of the NC Statewide Information Security Manual are included in the appendices of this document.

*** In 2012, Datatel and SunGard Systems merged, and changed their company name to Ellucian.

Chapter 1 Roles, Responsibilities and the separation of duties

This chapter defines the roles and responsibilities of the college IT Users as Data and Application owners versus those of the college IT Staff as support and service providers. The roles and responsibilities described are those required for the use, support and maintenance of the College's Ellucian System. For the purpose of this document, the term Ellucian System includes all Ellucian Colleague software and associated databases, and the hardware used to host those software applications. This includes the host server and all the additional hardware and software implemented by the college that interacts with that host server to deliver the tools and services necessary to conduct college business. Chapter 2 describes the Ellucian System and those coupled applications in more detail.

MIS Staff Roles and Responsibilities

The Ellucian System is administered by the System Administrator in Management Information Services. System Administration includes all of the activities required to implement, tune, maintain, upgrade, and secure the system. Some of the specific duties include:

Operating System Maintenance
Database Administration
User account and security Maintenance
Backups
Software Installation

Performance Monitoring and Tuning
Patch Installation
System Security
Hardware Maintenance

The System Administrator requires unrestricted access to the Ellucian system to perform the duties listed above; however, it is important to understand that unrestricted access does NOT imply that the Systems Administrator assumes any responsibilities for the maintenance of data or the execution of the software applications that exist on the Ellucian server to satisfy college business requirements. For example, the System Administrator will install the software patches required to keep the Payroll Processes up to date, create tape backups of the payroll data, and tune the database on a daily basis, but the System Administrator will NEVER run payroll processes, maintain payroll data, print checks, or generate reports from payroll data. That is the responsibility of the business unit that owns those processes and data. Database Administration is also the responsibility of the Systems Administrator and includes monitoring file sizes, efficiencies, and indexing as it applies to performance; however, the accuracy of the data stored in the Database is the responsibility of the users that are considered owners of the data. For example, if an employee or student address has been entered incorrectly, it is the responsibility of the office considered the owner of that data to handle the maintenance. The MIS department does not own any of the data stored in the Ellucian System.

All operating system level administration and maintenance is performed by the System Administrator. Access to the Operating System is limited to MIS staff only. As published in the Statewide Information Security Manual, Standard 020105, "Only those individuals designated as system administrators shall have access to operating system commands". Also, Standard 080101 states that, "Agencies shall restrict access to operating system and operational or production application/program libraries to designated staff only." This standard not only addresses the operating system, but also includes application/program libraries, which applies to the access and maintenance of Software used in the Colleague application. Application and program library access is limited to the Application Management (Programming) area of MIS. User areas are not permitted to have access to software development on the Ellucian System in any capacity per Standard 080101.

Owner roles and responsibilities

The Ellucian system is made up of thousands of processes that are used by all areas of the college to capture, maintain, and report data and information to satisfy college business requirements. The use of each of those processes is intended for the office or unit that is responsible for satisfying the requirement, such as the processes and data associated with the payroll function that are intended for the payroll department, while grade rosters processes are intended for the Curriculum and Continuing Education Registrars offices. When the determination is made that a process is intended for use by a specific office, that office is then considered the custodian or owner of that process and its associated data, and is responsible for the efficient, accurate and secure use of those processes and data. This is the basis used by the college for assigning all process ownership. Standard 010102 of the Statewide Information Security Manual states that in order to “Protect the College’s Information” each college must identify and maintain an inventory of all Information assets that includes identification of the custodian of each asset. A detailed Ellucian system process inventory and ownership assignments are provided in chapter 3 of this document as a response to this standard.

The college currently recognizes two owners, the Senior Vice President for Business and Finance and the Senior Vice President for Academic and Student Services. These owners are the members of senior management that are ultimately responsible for the use of the college’s data and processes. The Senior Vice President for Business and Finance is the owner of all College Finance and HR processes and their associated data, while the Senior Vice President for Academic and Student Services is responsible for the Student, Course and Academic Programs processes. Both owners have delegated ownership responsibilities to process custodians in each of their areas. A detailed description of this ownership hierarchy for each area is provided later in this chapter.

Owner responsibilities include but are not limited to managing usage, process and parameter setups, business workflows, staff training, user access authorizations, and security class management. In addition to the daily activities, owners are also responsible for the planning, testing and implementation of new software enhancements released by Ellucian and the NCCCS. This includes the testing and implementation of routine patches that are delivered on a weekly basis. Some of the specific duties and responsibilities that accompany data and application ownership include the following:

- Authorize or deny access to data and processes within their area of ownership by signature, to include the assignment of both user accounts and security classes.

- Disclose to users within their area College guidelines, procedures and policies governing the use of college computing resources.

- Publish departmental procedures, guidelines, and policies regarding the handling and release of all information.

- Publish data classification for area of ownership where data is rated by sensitivity, confidentiality, and value.

- Participate in the semi-annual review of all user access and access controls for their given application areas.

- Review methods for safeguarding information from unauthorized use, accidental and intentional alteration or destruction.

- Responsible for the accuracy, integrity and timeliness of processing.

- Responsible for the testing of specific system enhancements and patches to determine impact on existing business functions.

- Responsible for providing users with sufficient training in the use and protection of data and processes within their area of ownership.

- Responsible for the development and maintenance of workflow and process documentation.

- Responsible for the development of business continuity and recovery plans for their specific areas.

It is understood that the owners have assigned many of duties and responsibilities listed above to custodians or individuals in the departments where the specific business activities take place. These assignments are documented as such for IT Governance.   The duties and responsibilities being delegated, and the individual(s) assigned those duties and responsibilities must be identified. Custodians are usually responsible for specific departments or areas that exist under the owners, and are more involved in the day to day operation of those areas. Although many of the custodians are considered to be the subject matter experts in their given areas, there are cases in some of the larger departments where their expertise may be limited. In those cases, the custodians may designate stewards for specific areas and processes. Stewards are described later in this section.

Custodians may also be designated as security officers for their given areas by the data owners. Security officers are those individuals responsible for generating the user and security class maintenance forms for their areas using a software application provided by MIS. The designation of security officers must be coordinated with the MIS System Administrator. The role of the Security officer is described later in this document.

There are currently ~~five~~ six custodians that have been identified by the owners. The Associate VP for Student Services, the Associate VP for Curriculum Programs, and the Associate VP for Continuing Education were appointed by the Senior Vice President for Academic and Student Services. The ~~Controller~~ Associate VP for Business and Finance, Director of Student Accounts and Fiscal Controls, and Director of Disbursements~~and Director of Budgets and Financial Systems~~ were appointed by the Senior Vice President for Business and Finance. The table shown below provides a general overview of the ownership areas for each of these custodians.

Custodian	Area of responsibility
Associate VP for Student Services	Curriculum Student Data
Associate VP for Curriculum Programs	Curriculum Course and Academic Program Data
Associate VP for Continuing Education	Continuing Education and Basic Skills Student, Course, and Academic Program data.
~~Controller~~Associate VP for Business and Finance	~~Accounts Payable, Accounts Receivable, Payroll, Grants and Loans,~~ Procurement, Budgets, Facility Services, Property Control
Director of ~~Budgets and Financial Systems~~ Student Accounts and Fiscal Controls	~~Property Control, Facility Services, Budgets~~Accounts Receivable and Grants and Loans
Director of Disbursements	Accounts Payable and Payroll/Benefits

All ~~five~~ six of these custodians have been assigned most if not all of the ownership duties for their specific areas, to include all decision making regarding the authorization or denial of access to processes and data within their functional areas. This is important as all access of Ellucian data and processes must be approved by signature of the owner of the requested resource. MIS will only accept user and security maintenance request that have been signed by the Senior Vice Presidents or one of these custodians as the owners. The Office of the State Auditors will pull a random sample of authorization forms during each FTE, Finance, and IT audit to verify that the correct owners have signed and authorized user access, based on the inventory and ownership published in this document.

The custodians, under the direction of the owners, are responsible for the timely and efficient use of the Ellucian System in their given areas in support of college business requirements and objectives. This includes maintaining workflow documentation and training materials. The custodians are also responsible for the testing and approval of all patches and enhancements. Because of the size and diversity of the functions and departments that exist within these areas, the custodians must rely on existing staff in those areas to perform many of these duties. Those staff or stewards are relied upon to perform owner duties specific to their business function. Stewards are involved with patch testing, user training, documentation, and daily use of the Ellucian system within their given areas. An example of a steward would be the Financial Aid Director under the Associate Vice President for Student Services.

Stewards are identified by the custodians, and may be assigned some of the duties of the custodians; however their role in the authorization and denial of access to processes and data is limited to making recommendations to the custodians and owners. The Stewards are considered the subject matter experts for their given areas and have working knowledge of the business processes used in their given areas. Stewards are usually involved with the testing and approval of patches, enhancements, implementation of new functionality, and training of new users within their departments. The following is a list of current stewards:

Dean of Enrollment Management

Accounts Receivable Manager

Financial Aid Director

Curriculum Registrar

Director of Counseling Services

Continuing Education Registrar

Director of Basic Skills

~~Accounting Manager~~State, County, and Grants Funds Manager

Payroll and Benefits Supervisor

Procurement and Special Projects Manager

Property Control & Services Supervisor

Director of Facility Services

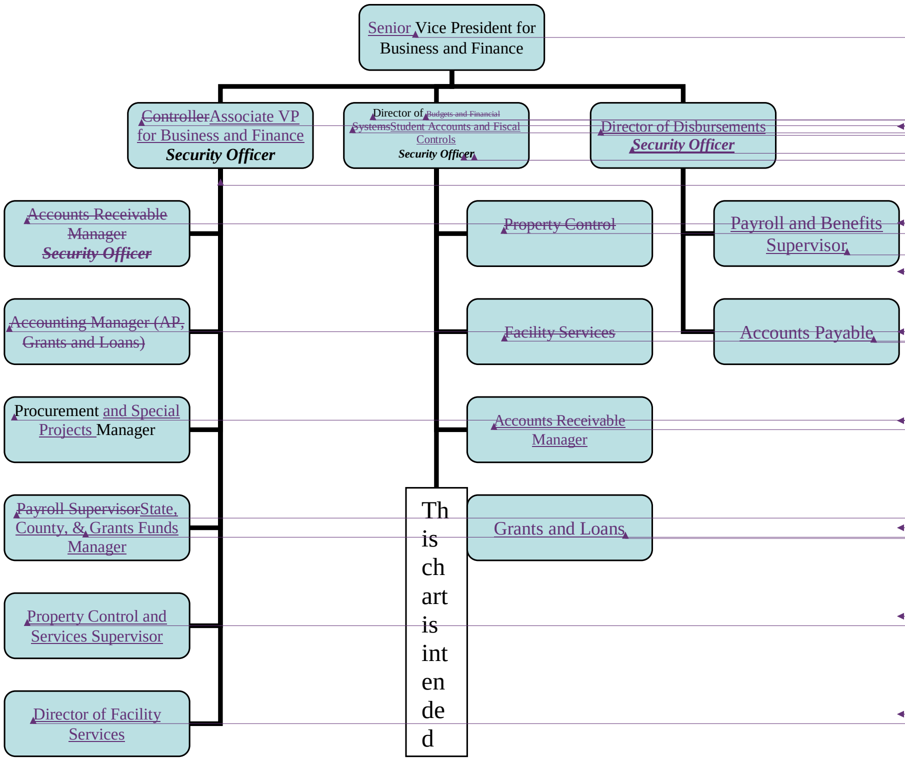
One of the most important responsibilities that owners have is deciding how to secure the data and processes that they own, and who will be allowed to have access to those processes and data, and in what capacity.   Owners must approve all access of Ellucian processes and data, both the access requested by users that work under them and users that work under other owners. Managing this access can be very complex and time consuming (covered in detail in Chapter 4). For that reason, the owners can appoint one of their custodians or stewards to also serve as the Security Officer for their area. Selection of these individuals must be coordinated with MIS and named in this documentation. These individuals are authorized to handle all of the paperwork necessary to request the addition, deletion, and maintenance of user accounts and security controls for their given areas. Each security officer will be provided with a software application that serves as a tool to assist them in the management of their users and security controls.   The security officers work closely with the MIS Systems Administrator.

Currently there are 7 security officers currently identified. ~~.~~ In the Business and Finance area, ~~both~~ Custodians (the ~~Controller~~ Associate VP for Business and Finance, Director of Student Accounts and Fiscal Controls, and Director of Disbursements~~and the Director of Budgets and Financial Systems~~) have chosen to assume the role of Security officer for their areas~~, with one exception~~. ~~Under the Controller, the Accounts Receivable Manager (Steward for that area) has been assigned the Security Officer role for AR user accounts and Security.~~ In the Academic and Student Services area, the Associate VP for Student Services and Associate VP for Curriculum Programs have chosen to assume the Security Officer roles, while the Associate VP for Continuing Education has delegated the Security officer responsibilities to the Continuing Education Registrar and the Director of Basic Skills in the Academic areas.

Ownership Hierarchy

As described in the previous section, ownership can be depicted as an organizational structure that identifies the owners, their appointed custodians and stewards (see chart below and next page). This ownership hierarchy will not match the organizational hierarchy, but does clearly define the delegation of ownership duties by the owners.   More importantly, it also defines each of areas and sub-areas of the college that are responsible for the execution of the business processes provided by the Ellucian system.

Those defined areas and sub-areas of the college and the MIS department are collectively responsible for the overall security of all the Data and Applications on the Ellucian server.


Senior Vice President for Business and Finance
~~Controller~~Associate VP for Business and Finance
Security Officer
Director of ~~Budgets and Financial Systems~~Student Accounts and Fiscal Controls
Security Officer
Director of Disbursements
Security Officer
~~Accounts Receivable Manager~~
~~Security Officer~~
~~Accounting Manager (AP, Grants and Loans)~~
Procurement and Special Projects Manager
~~Payroll Supervisor~~State, County, & Grants Funds Manager
Property Control and Services Supervisor
Director of Facility Services
~~Property Control~~
~~Facility Services~~
Accounts Receivable Manager
This chart is intended
Grants and Loans
Payroll and Benefits Supervisor
Accounts Payable

Formatted: Font: 8 pt

Formatted: Font: 8 pt

Formatted: Font: 5.5 pt

Formatted: Font: 4 pt

Formatted: Font: 7.5 pt

Formatted: Centered

Formatted: Font: 5.5 pt

Formatted: Font: 7.5 pt, Bold, Italic

Formatted: Font: 6 pt

Formatted: Font: 8 pt

Formatted: Font: 9 pt

Formatted: Font: 8 pt

Formatted: Centered

Formatted: Font: 8 pt

Formatted: Font: 9 pt

Formatted: Left

Formatted: Font: 8 pt

Formatted: Centered

Formatted: Font: 9 pt

Formatted: Font: 8 pt

Formatted: Font: 8 pt

Formatted: Font: 7.5 pt

Formatted: Centered

Formatted: Font: 8 pt

Formatted: Centered

Formatted: Font: 9 pt

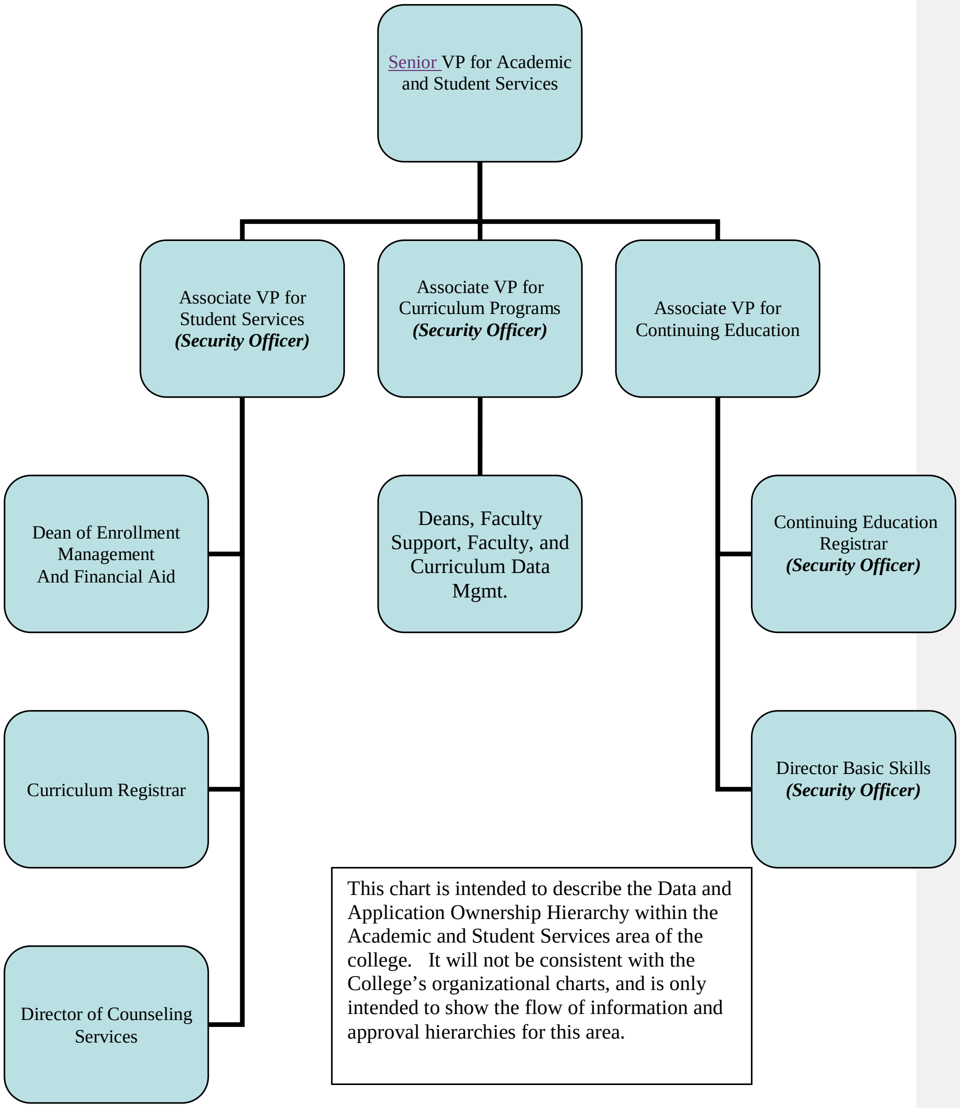
Formatted: Font: 8 pt

Formatted: Font: 8 pt

Formatted: Centered

Formatted: Font: 8 pt

Formatted: Centered


Senior VP for Academic and Student Services
Associate VP for Student Services *(Security Officer)*
Associate VP for Curriculum Programs *(Security Officer)*
Associate VP for Continuing Education
Dean of Enrollment Management And Financial Aid
Curriculum Registrar
Director of Counseling Services
Deans, Faculty Support, Faculty, and Curriculum Data Mgmt.
Continuing Education Registrar *(Security Officer)*
Director Basic Skills *(Security Officer)*

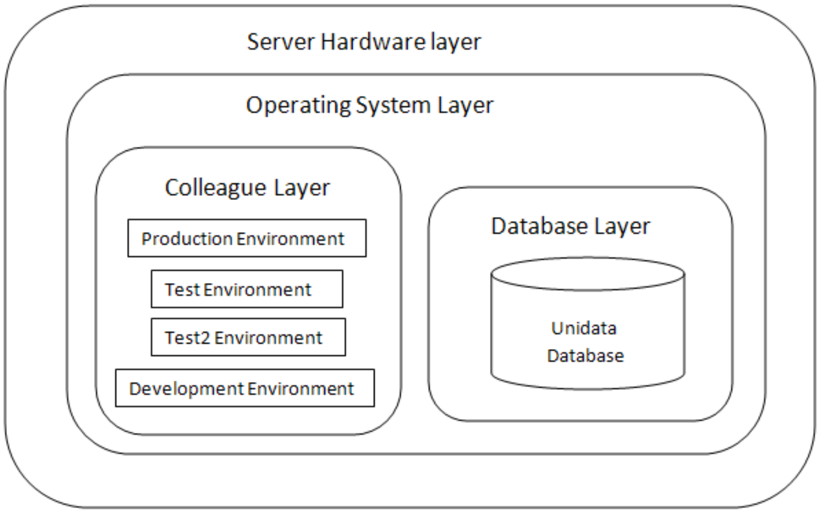
This chart is intended to describe the Data and Application Ownership Hierarchy within the Academic and Student Services area of the college. It will not be consistent with the College's organizational charts, and is only intended to show the flow of information and approval hierarchies for this area.

Chapter 2 Colleague Structure and Components overview

As presented in chapter one, every process included in Ellucian's Colleague software has an owner or custodian assigned to it that is responsible for it's secure, accurate, and efficient use. There are thousands of processes included with the Colleague software, making management of process inventories and ownership assignment both complex and cumbersome, especially if the process is shared by multiple departments and is "co-owned". This chapter will focus on ownership of the Colleague software as a whole and will begin to define the scope of ownership from a much broader perspective. Chapter 3 will focus on ownership specifics.

When an owner is assigned to a process, they need to understand that the process they own is a component of one of the five Colleague business applications, and those five applications are the Colleague system.   The Colleague System resides on server hardware and must rely on the database application and operating system on the server in order to function.   It is important to recognize these dependencies, as ownership roles and responsibilities cannot be limited to just processes. When an owner authorizes a user to access a process, they are authorizing this user to access the server hardware and use of the operating system and database as the process cannot run with them.

The diagram on the next page is a depiction of the dependencies or layers mentioned above, with the Server hardware being the outermost layer and the Colleague software and Database as the innermost layers. In the diagram, the Colleague software layer shows 4 environments. For the purpose of this diagram, consider each environment as a separate version of the Colleague software. Environments are explained later in this section. In the diagram, Colleague processes reside in the inside the environments of the Colleague software layer. The only way to get to the processes is by passing through those outer layers.



The Server Hardware layer is a server located on the college's intranet, and is accessible using approved client applications or by accessing front end applications that access the server. The tools used to connect to the hardware are discussed after this section.

The operating system layer is the software that makes the server run. It also acts as host for all other software applications that run on the server. An example of an operating system would be the Windows operating system found on most personal computers. Windows can host many software applications such as WordPerfect or Microsoft Office. The operating system used by the college to host the Ellucian Colleague Software on an Oracle (formerly Sun) server is Unix, and it is the software that processes user login id's and passwords, password expiration, general system security, printed output routing, communication management email and the physical reading and writing of data in the Ellucian Software Application. Every user that access the colleague server will indirectly interact with the Operating System; however access to the Operating System parameters, setups, and commands is restricted to the MIS Systems Administration Staff only as required by Standard 020105 of the Statewide Information Security Manual.

The database layer is the software application that handles the physical creation, organization, modification and access of data stored on a computer system. Rocket's (formerly owned by IBM) Unidata software is the database management system used by the college.   It is used by the Colleague software for the storage, maintenance and retrieval of all data. Users communicate indirectly with the database management system using the Colleague processes and the Informer reporting tools.

The Colleague Software layer is where all the processes reside.   These are the processes that all users interact with to capture, input, process, and output data from the Colleague and the Database, as required to satisfy college business needs.   The Colleague software must interact with the Operating System and Database Management System on the server hardware to perform all tasks while interacting with users through a user friendly GUI (connectivity tools discussed later).

As shown in the previous diagram, there are 4 environments listed in the Colleague Software layer. Each of the environments listed is a complete set of all of the Colleague software applications and data. Environments allow the college to build testing, training, and development versions of Colleague that can be used for those purposes without risking loss or damage of the college's production data. The college's environments are Production, Test, Test2 and Development.   The production environment has the current version of all data and Colleague software being used by the college to meet business objectives. Access to the production environment must be authorized by the data owners.   The test and test2 environments, as the name implies, are "workspaces" that all users can use to test, practice or train without any risk to production data. The test environments include all the Colleague Software, to include newly released enhancements and patches not yet loaded into production, and copies of all the data files from the production environment. The data in the test environments can be refreshed from the production data at the request of the data owners. Ellucian and System Office patches will always be loaded into the test environments first, and will not be loaded into Production until the Data Owners have tested the changes.   The Development environment is reserved for use by the MIS programmers.

Most of the ownership responsibilities outside of the MIS department pertain directly to the Ellucian Software layer, but owners should also be aware of the indirect interaction that their users have on the database and operating system when they use the Ellucian software. When an owner authorizes a user to access an Ellucian Process, that user is also authorized to interact with everything that process might interact with on the system.

Colleague connectivity tools

The previous discussion describes the Colleague software and Unidata Database as being hosted on a server running the UNIX operating system. What hasn't been addressed is connectivity to the server. In order to run and interact with Colleague processes, a user has to connect to the server using approved software on a workstation connected to the intranet or internet. Just as described with the layers, ownership roles and responsibilities also apply to connectivity.

If a user must have access to Colleague so that they can run business processes, they will have to use the UIWeb interface. If a user needs to access the Colleague Self Service applications, they must connect to the server using the WebAdvisor interface. Both interfaces provide access to Colleague processes; however when using WebAdvisor the user is limited to viewing and processing information for and about their selves only, based on the ID that they use when they log in. For example, a Faculty member will use UIWeb to register students, print rosters, enter grades, and retrieve information about their advisees. If that same faculty member wants to view an image of their Pay Advice or W2, or look at their personal transcript, they would log in using WebAdvisor. While in WebAdvisor, the user cannot access any records other than their own.

Both interfaces require a login and password that are presented to the Colleague software through the Operating and Database management systems. Once logged in, the users are granted access to the Ellucian processes and mnemonics that they are authorized to use by their supervisors and the process owners. Access is assigned based on the login id used.

Both interfaces are Web based meaning that they are accessed and run using a Web Browser, such as Internet Explorer, Firefox, or Google Chrome. Access to the Colleague server using UIWeb is limited to the intranet (must be on the FTCC campus network), while WebAdvisor is available from anywhere. Use of UIWeb is limited to employees of the college while WebAdvisor is available to guests, prospects, applicants, students, alumni and employees.

Database connectivity

Another interface that is available to users is Informer, which is a reporting tool that allows users to generate Ad-hoc reports and data analysis from the data stored on the Colleague server. This interface does not allow users to interact will the Colleague software. Instead, users connect to and interact with Informer software that resides on a separate server, using a web browser. The Informer software will present report parameters and selection criteria supplied by the user to the Unidata Database and return the information as output in a variety of formats to the user submitting the request. Access to Informer is limited to employees of the college and is only available from the intranet. Data owners must authorize access to their data for each user.

Coupled Systems

UIWeb, WebAdvisor, and Informer are all tools that allow users to communicate with the Colleague software applications and data. There are also processes that interact with the Colleague Software that are not initiated or driven by user requests. Instead, they are servers and applications that automatically send and receive data to and from the Colleague Server based on activities, triggers and events defined by business rules of the college. These servers and their associated software are referred to as coupled systems.

Each of these coupled systems was implemented to satisfy a specific business requirement of the college. The MIS Systems Administrator role with these systems will be limited to server setup, maintenance, security, and performance. The owners responsible for the business processes running on those servers will be responsible for business workflow configurations and setups, data integrity, and timeliness of processing.

Currently, the coupled systems and applications are CFNC Mentor, Accuplacer, and Eprocurement, and the SOFTDOCS applications. It is important for the Data/Application owners to understand the role and capabilities of these systems, as many of the Data and Application ownership responsibilities and duties apply to them even though they are physically separate from the Colleague software. The following is a brief description of each.

CFNC Feeds (College Foundation of North Carolina)

The College Foundation of North Carolina (CFNC) is a free service of the State of North Carolina that helps students plan, apply, and pay for college. One of the key features of this service provides potential students with the ability to complete a standard application at the CFNC.org web site, and then have it submitted electronically to the NC Universities and Colleges that they choose. The primary source for all FTCC application data is from the CFNC.org web site. As potential students apply at the CFNC web site, applications are sent to the college electronically and received by a small server dedicated to this purpose. Applications are then automatically uploaded from this server to the Colleague Application processes on scheduled intervals. At that point the data is stored on our local Colleague Server as Admissions data, and is owned by the Associate Vice President for Student Services. It is important to understand that those ownership responsibilities are not limited to the data after it is received by the college. The Associate Vice President for Student Services has staff that is responsible for the FTCC application parameters at the CFNC web site and has a secure login to that site for this purpose. That staff is also responsible for maintaining the local Colleague parameters and settings that define how application data is loaded so that it is consistent college business practices.

Accuplacer Feed

Another system that automatically feeds data to the Colleague server is the Accuplacer feed. This is an application that is hosted on a separate server located on the college local network. As students complete admissions testing, the tests are automatically scored and the results are sent to the Accuplacer server. This server is dedicated to this purpose. Once the data is placed on this server, it is automatically uploaded into the Colleague system based on parameters maintained by the college testing and admissions functions.   Ownership responsibilities for these processes extend beyond the scope of the Colleague server.

Eprocurement

The Eprocurement application is hosted on a separate server and is used by the Ellucian system to communicate with NC@your service. This application receives electronic requisitions from the Ariba Eprocurement site and submits them to the Ellucian server for processing. Once a requisition is processed and approved on the Ellucian system, a purchase order will be generated and sent to the Eprocurement application where it will electronically dispatched to the supplier. This application will also process new vendors into local files as they register on the state site. Users are not permitted direct access to this system.

Softdocs printing/scanning

The SOFTDOCS printing application runs on a separate server and is used to format printed output for specialized printing on laser printers, such as official transcripts and rosters. It is the laser print solution utilized by the non financial users.   End users do not log into this system. Output is directed to this system for printing by users when they identify “aigstream” as the printer to be used when running Ellucian processes that generate printed output. The SOFTDOCS scanning application runs on the same server as the print solution, and is used by some departments to scan and store documentation provided by students.   Scanned data is stored on the SOFTDOCS server in folders using the students Ellucian id as the folder name.

FTP, Easy Spooler, Source 4

FTP, or file transfer protocol, is a network protocol used to transfer files from one computer to another through a network. Typically, one computer will function as an ftp server and handle data transfer requests from ftp clients running on other computers. In our case, the Ellucian Server is the ftp server for local data transfers, and users run an ftp client on their desktop to retrieve data to their workstation to satisfy some sort of electronic reporting requirement. The college currently uses Ipswich WS-FTP as the client, which is installed and configured on individual desktops by MIS technicians. The data owners and/or designees for each area of the college must authorize ftp usage for every user, as it is a restricted application.

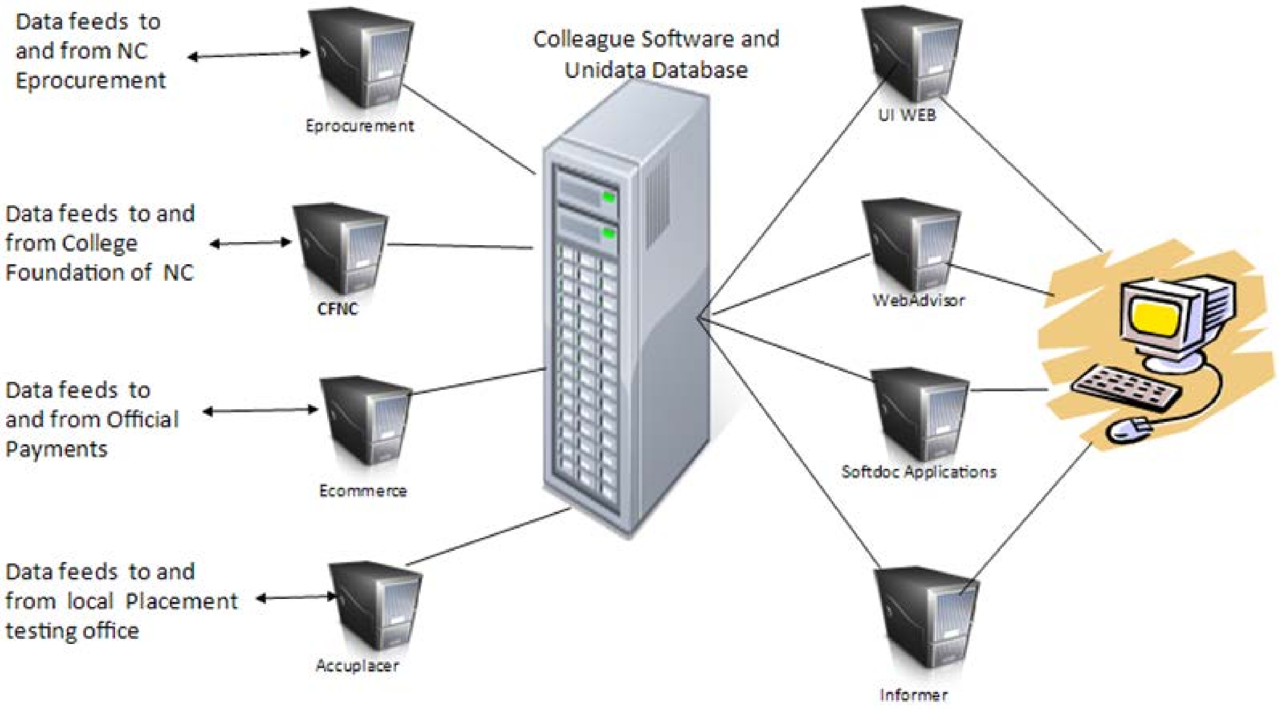
Easy Spooler is a software application on the Ellucian server that handles all Ellucian printing. The Ellucian Colleague application does not have print capabilities, but instead builds print images at the Operating System level that are retrieved by Easy Spooler and printed.

Source 4 is a software application on the Ellucian server that formats printed output for specialized printing on laser printers. Unlike the SOFTDOCS laser printing solution, the formatting is done on the Ellucian server and sent directly to the printer. It is considered the laser print solution for the Financials area, and is used to generate checks, purchase orders, pay advices, W2's, etc. The Easy Spooler application will redirect printed output to Source 4 for formatting prior to sending the information to a printer. The North Carolina Community College System office has directed all colleges to move all Source 4 laser print output to Softdocs, as Source 4 will not be supported after 2014.

Summary

As mentioned in chapter 1, the term Ellucian System is the logical application entity that is physically comprised of a host server running Colleague Software and Unidata database, and specialized software applications that are loosely coupled to the Ellucian application. Loosely coupled applications are hosted on separate servers and include Eprocurement, WebAdvisor, UI Web, Ecommerce, NC Mentor, Informer, SOFTDOCS (Scanning, Printing, and Document capture), and Accuplacer. All of the physical components that make up this logical entity have to be considered when assigning ownership responsibilities and duties.

On the following page is a diagram that summarizes the current implementation at FTCC, identifying each of the components of the overall system.


Data feeds to and from NC Eprocurement
Eprocurement
Colleague Software and Unidata Database
UI WEB
Data feeds to and from College Foundation of NC
CFNC
WebAdvisor
Data feeds to and from Official Payments
Ecommerce
Softdoc Applications
Data feeds to and from local Placement testing office
Accuplacer
Informer

Chapter 3 Assignment of Colleague Application Ownership

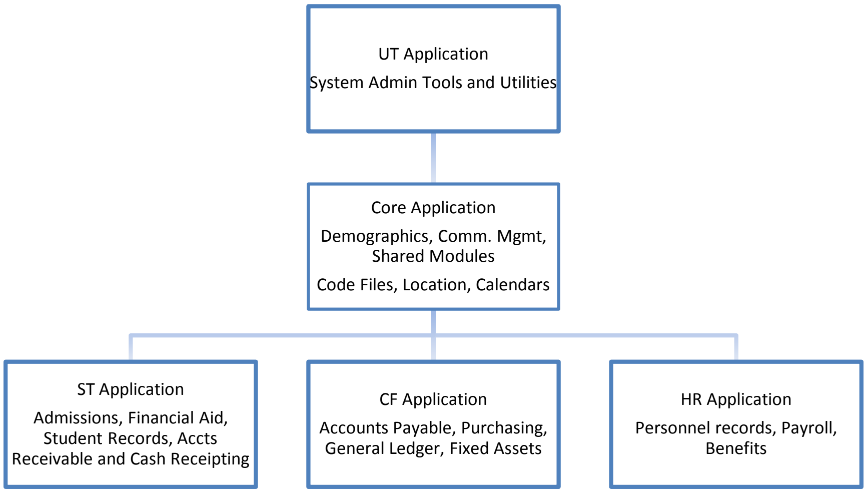
As mentioned in chapter 2, the Ellucian Colleague Software is installed multiple times in separate areas called environments. They are named Production, Test, Test2, and Development. Included in each of those environments are complete sets of the software and data base files. The role of each environment can be derived from the name assigned to it. The Production environment is where all of the current software and data reside that is required by the college to satisfy all business requirements. The Test and Test2 environments are used to support the testing and training requirements of the college (see chapter 5 for information regarding the testing of Patches and enhancements). The Development environment is reserved for the MIS programmers and third party vendors that have been contracted to develop software. With the exception of Development, Environments are considered “co-owned” and shared by the Owners; while specific ownership responsibilities within each environment are assigned based on the applications. This chapter will focus on the assignment of process and application ownership within the environments, and will provide a detailed inventory of all Colleague software applications, processes, modules, etc. that includes ownership assignments.

In chapter 2, it was stated that Colleague processes are components of the 5 applications that make up the Colleague Software. Ellucian defines Colleague as a suite of applications, and each application is a collection of modules grouped together to meet the needs of a broad functional area. Each module is then made up of individual processes designed to address a specific business function of the module.

There 5 applications included in the Colleague Software are:

- Utilities (UT)
- Core System (CORE)
- Colleague Financials (CF)
- Student System (ST)
- Human Resources (HR)

Each of the application is related to each other and in some cases dependent on each other to function.   This relationship is called the application hierarchy or tree (see figure below). In Colleague, the Student, Human Resources, and Financial Systems are at the bottom of the tree structure and are parallel to one another. Applications at the same level are referred to as peer applications.


UT Application
System Admin Tools and Utilities
Core Application
Demographics, Comm. Mgmt, Shared Modules
Code Files, Location, Calendars
ST Application
Admissions, Financial Aid, Student Records, Accts Receivable and Cash Receipting
CF Application
Accounts Payable, Purchasing, General Ledger, Fixed Assets
HR Application
Personnel records, Payroll, Benefits

Each of the applications includes the modules and data that are specific to that application, and can readily share data and modules with an application that is above it in the hierarchy. For example, the HR application includes the data and modules necessary to run a Payroll, but shares the demographics module in CORE with the ST and CF applications to maintain Employee demographic data.   When a lower application uses modules stored in a higher application, it is transparent to the end user. If a module does not exist in the application, Colleague searches up the application tree to find the program that it needs. Colleague will never search down or across the application tree for programs.   This search method allows the CORE application to house many of the modules and data that are common to and shared by the CF, HR, and ST applications, such as communication management, demographic data for all students and employees, facilities, semester schedules and calendars.

The UT application positioned at the top of the tree is also shared by the lower applications to perform many of the technical tasks and System Administration functions.

At first glance, it would appear that ownership could be easily assigned at application level, and apply to each of the modules and process contained within them, but there are two issues that prevent this. First, both Senior Vice Presidents have chosen to delegate ownership responsibilities for specific modules to different custodians in their areas. Although the Senior Vice Presidents still have overall ownership responsibilities, the custodians are named as the owner designee for those specific modules. Second, the overall ownership responsibilities of the Student application cannot be assigned to either Senior Vice President, as both own modules in the application. The CORE application is also shared by all areas of the college.

As described earlier, there are five Colleague applications (UT, CORE, CF, HR, ST) in each of the environments (Production, Test, Test2, Development). Each of those applications is broken down into modules, and each module is made up of menus, submenus and processes. Shown on the next page are tables that identify each module included in the CORE, CF, HR, and ST applications. The UT application is not included as it is owned and used by the MIS Systems Administrator and staff. Use of the UT modules and processes is limited to the Systems Administration staff.

As shown in the table, each module addresses a business function of the college that is specific to a business unit, department or division of the college. Some of the modules are very specific to a single business function, while others are designed to address a group of similar functions. In some cases modules are shared by multiple areas of the college. For example, the RG or Registration module is shared by the Curriculum, Continuing Education, and Basic Skills areas of the college.

Core Application Core Application modules	Financial Application CF Application modules	Human Resources Application HR Application modules
DM Person Demographics	AP Accounts Payable	PE Personnel
OR Organization Information	BU Budget Management	PR Payroll
FP Facilities Profile	FX Fixed Assets	PC Position Budgeting
CC Communications Management	GL General Ledger	ER Employee and Labor Relations
SC Scheduling	IN Inventory	CC Communications Management
AE Activities and Events	PI Pooled Investments	HD Human Resources Data Marts
SV Staff/Volunteer Information	PP Physical Plant	XHRM Custom Human Resources
PH Process Handler	PU Purchasing	WB Web Admin Support
ELF Electronic File Transfers	PA Projects Accounting	
SP Sponsored Projects	XFM Custom Financial System	
EC E-Commerce	CC Communications Management	
CS Core Setup/Utilities		
XCOM Custom Core System		

Colleague Student Application (ST)		
AC Academic Records	DM Person Demographics	WB WEB Admin Support
AM Recruitment/Admissions Mgmt	FA Financial Aid	SDU Student Database Utilities
AR Accounts Receivable	FRP Federal Reporting	SMO Suggested Menu Options
CO Campus Organizations	SRS State/Provincial Reporting	R25 RESOURCE25 Interface
CR Cash Receipts	FO Forms Processing	S25 SCHEDULE25 Interface
CU Curriculum Management	FI Faculty Information	SSS Student System Setup
DA Degree Audit	RG Registration	XSTM Custom Student System

On the following pages is a detailed inventory of each Colleague application. In that inventory, each module is listed along with the module's primary user, custodian, and individuals that have the responsibility to authorize or deny access to the module and its associated data. These lists represent the inventory of all Colleague process and associated data assets used by the college to satisfy business needs and requirements.

Module ownership was determined by identifying the business unit responsible for the execution of the module provided. Key Users, Custodians and designees were identified by the Senior Vice

Presidents. In many cases modules in the ST application are shared by multiple areas of the college.   All primary users, custodians and designees are identified in those cases. An example would be the Registration Processes that are owned by the Senior VP for Academic and Student Services. These processes are shared by Continuing Education, Basic Skills and Curriculum areas of the college.

Colleague Core Applications (CORE)

Application/Data Owners - This application houses all of the common applications shared by all users.

Core Application modules	Primary/Functional user	Custodian	Data/Application Owner and designees authorized to approve and deny access
DM Person Demographics	Shared (Core Team)	Based on application area	Based on application area
OR Organization Information	Shared (Core Team)	Based on application area	Based on application area
FP Facilities Profile	Director of Facility Services	Based on application area	Based on application area
CC Communications Management	Shared (Core Team)	Based on application area	Based on application area
SC Scheduling	Curriculum Data Mgmt		
AE Activities and Events	Not used		
SV Staff/Volunteer Information	MIS	MIS	
SL Surveys			
PH Process Handler	MIS	MIS	
ELF ELectronic File Transfers	MIS	MIS	
SP Sponsored Projects	Not implemented	MIS	
EC E-Commerce	~~Controller~~Procurement and Special Projects Manager	~~Controller~~Associate VP for Business and Finance	Senior VP for Business and Finance ~~Controller~~Associate VP for Business and Finance
MOB Datatel Mobility	Not implemented	MIS	
CS Core Setup/Utilities	Shared (Core Team)	MIS	
XCOM Custom Core System	Shared (Core Team)	MIS	

Colleague Financial Applications (CF)

Application/Data Owner: Senior Vice President of Business and Finance
CF Security Custodian: Financial Systems & Disbursement Manager

CF Application modules	Primary/Functional user	Custodian	Data/Application Owner and designees authorized to approve and deny access
AP Accounts Payable	~~Accounting Manager~~ Director of Disbursements	~~Controller~~Director of Disbursements	Senior Vice President of Business & Finance ~~Controller~~Associate VP for Business and Finance
BU Budget Management	~~Director of Budgets & Financial Systems~~State, County, and Grants Funds Manager	~~Director of Budgets & Financial Systems~~Associate VP for Business and Finance	Senior Vice President of Business & Finance ~~Controller~~Associate VP for Business and Finance
FX Fixed Assets	Property Control & Services Supervisor	~~Director of Budgets & Financial Systems~~Associate VP for Business and Finance	Senior Vice President of Business & Finance ~~Controller~~ Associate VP for Business and Finance
GL General Ledger	~~Director of Budgets & Financial Systems~~Shared	~~Director of Budgets & Financial Systems~~ Associate VP for Business and Finance	Senior Vice President of Business & Finance ~~Controller~~Associate VP for Business and Finance
IN Inventory	Director of Facility Services	~~Director of Budgets & Financial Systems~~Associate VP for Business and Finance	Senior Vice President of Business & Finance ~~Controller~~Associate VP for Business and Finance
PI Pooled Investments	~~Director of Budgets & Financial Systems~~State, County, and Grants Funds Manager	~~Director of Budgets & Financial Systems~~Associate VP for Business and Finance	Senior Vice President of Business & Finance ~~Controller~~Associate VP for Business and Finance
PP Physical Plant	Director of Facility Services	~~Director of Budgets & Financial Systems~~Associate VP for Business and Finance	Senior Vice President of Business & Finance ~~Controller~~Associate VP for Business and Finance
PU Purchasing	Procurement and Special Projects Manager	~~Controller~~Associate VP for Business and Finance	Senior Vice President of Business & Finance ~~Controller~~Associate VP for Business and Finance
PA Projects Accounting	~~Director of Budgets & Financial Systems~~State, County, and Grants Funds Manager	~~Director of Budgets & Financial Systems~~Associate VP for Business and Finance	Senior Vice President of Business & Finance ~~Controller~~Associate VP for Business and Finance
XFM Custom Financial System	Shared	~~Controller, Director of Budgets & Financial Systems~~Associate VP for Business and Finance, Director of Student Accounts and Fiscal Controls, Director of Disbursements	Senior Vice President of Business & Finance ~~Controller~~Associate VP for Business and Finance
CC Comm Mgmt	Shared	~~Controller, Director of Budgets & Financial Systems~~Associate VP for Business and Finance, Director of Student	Senior Vice President of Business & Finance ~~Controller~~Associate VP for Business and Finance

		Accounts and Fiscal Controls, Director of Disbursements	

Colleague Human Resources Applications (HR)

Application/Data Owner: Senior Vice President of Business and Finance

HR Security Designee: Financial Systems & Disbursement Manager

HR Application modules	Primary/Functional user	Custodian	Data/Application Owner and designees authorized to approve and deny access
PE Personnel	Payroll and Benefits Supervisor	~~Controller~~Director of Disbursements	Senior Vice President of Business & Finance ~~Controller~~Associate VP for Business and Finance
PR Payroll	Payroll and Benefits Supervisor	~~Controller~~Director of Disbursements	Senior Vice President of Business & Finance ~~Controller~~Associate VP for Business and Finance
PC Position Budgeting	Payroll and Benefits Supervisor	~~Controller~~Director of Disbursements	Senior Vice President of Business & Finance ~~Controller~~Associate VP for Business and Finance
ER Employee and Labor Relations	Payroll and Benefits Supervisor	~~Controller~~Director of Disbursements	Senior Vice President of Business & Finance ~~Controller~~Associate VP for Business and Finance
CC Communications Management	Payroll and Benefits Supervisor	~~Controller~~Director of Disbursements	Senior Vice President of Business & Finance ~~Controller~~Associate VP for Business and Finance
HD Human Resources Data Marts	Payroll and Benefits Supervisor	~~Controller~~Director of Disbursements	Senior Vice President of Business & Finance ~~Controller~~Associate VP for Business and Finance
XHRM Custom Human Resources	Payroll and Benefits Supervisor	~~Controller~~Director of Disbursements	Senior Vice President of Business & Finance ~~Controller~~Associate VP for Business and Finance
WB Web Admin Support	Payroll and Benefits Supervisor	~~Controller~~Director of Disbursements	Senior Vice President of Business & Finance ~~Controller~~Associate VP for Business and Finance

Colleague Student Application (ST)

Non AR Application/Data Owner: Senior Vice President for Academic and Student Services

AR/CR Application/Data Owner: Senior Vice President of Business and Finance

CU Student Services Custodian: Associate VP for Student Services
Stewards: Curr Registrar, Finanancial Aid Director,

CU Curr Programs, Courses Custodian: Associate VP for Curriculum Programs

CE Student Services Custodian: Associate VP for Continuing Education
Stewards: CE Registrar

Basic Skills Program Custodian: Associate VP for Continuing Education
Steward: Director of Basic Skills

AR/CR Custodian: Controller
Steward: AR Manager

ST Application modules	Stewards	Custodians	Data/Application Owner & designees authorized to approve and deny access
AC Academic Records	CU Registrar CE Registrar Basic Skills staff	AVP Student Services AVP Continuing Education Basic Skills Director	Senior VP for Academic & Student Services Assoc VP Student Services Assoc. VP for CE
AM Recruitment & Admissions Mgmt	CU Registrar CE Registrar Basic Skills staff	AVP Student Services AVP Continuing Education Basic Skills Director	Senior VP for Academic & Student Services Assoc VP Student Services Assoc. VP for CE
AR Accounts Receivable	AR Manager	~~Controller~~Director of Student Accounts and Fiscal Controls	Senior VP of Business & Finance ~~Controller~~Associate VP for Business and Finance
CO Campus Organizations	Shared	Shared	Any ST Owner or Custodian
CR Cash Receipts	AR Manager	~~Controller~~Director of Student Accounts and Fiscal Controls	Senior VP of Business and Finance ~~Controller~~Associate VP for Business and Finance
CU Curriculum Management	CU Data Mgmt CE Registrar	AVP Student Services AVP Curr Programs AVP Continuing Education Basic Skills Director	Senior VP for Academic & Student Services AVP for Curr Programs Assoc VP Student Services Assoc. VP for CE
DA Degree Audit	CU Registrar CE Registrar	AVP Student Services AVP Continuing Education	Senior VP for Academic & Student Services AVP Student Services AVP for CE
DM Person Demographics	Shared	Shared	Senior VP for Academic & Student Services AVP Student Services AVP for CE
FA Financial Aid	Financial Aid Director	AVP Student Services	Senior VP for Academic & Student Services AVP Student Services
FRP Federal Reporting	AR Manager (1098) Financial Aid Director CU Data Mgmt (IPEDS)	AVP Student Services ~~Controller~~Director of Student Accounts and	Senior VP for Academic & Student Services AVP Student Services

		Fiscal Controls	AVP for CE
FI Faculty Information	CU Data Mgmt Technician CE Registrar	AVP Student Services AVP Continuing Education Basic Skills Director	Senior VP for Academic & Student Services AVP Student Services AVP for CE
RG Registration	CU Registrar CE Registrar Basic Skills staff	AVP Student Services AVP Continuing Education Basic Skills Director	Senior VP for Academic & Student Services AVP Student Services AVP for CE
WB WEB Admin Support	Shared	Shared	Senior VP for Academic & Student Services AVP Student Services AVP for CE
SDU Student Database Utilities	Shared	Shared	Senior VP for Academic & Student Services AVP Student Services AVP for CE
SMO Suggested Menu Options	Shared	Shared	Senior VP for Academic & Student Services AVP Student Services AVP for CE
SSS Student System Setup	Shared	Shared	Senior VP for Academic & Student Services AVP Student Services AVP for CE
XSTM Custom Student System	Shared	Shared	Senior VP for Academic & Student Services AVP Student Services AVP for CE

Chapter 4 Granting, Managing and Securing Access

As described in Chapter 2 of the Statewide Information Security Manual, colleges are required to develop standards to control the use of the colleges technology assets and resources to include:

The colleges Network
All devices connected to the college's network
All Information assets available on the college network
Business applications (Email, Colleague Software)
Internet service provided by the college

The procedures and standards developed by the college to control the use and access of the resources listed above are published in Section I-23.10 of the college's Administrative Procedures manual, and apply to ALL college technology users. Owners and their appointed custodians must ensure that each technology user in their area is aware of these standards. While the intent of this document is to address IT Governance as it applies to the use of the Ellucian Colleague software, it is important to recognize that the use of the Colleague software is dependent on each of the resources listed. A user must have access to a device attached to the college network in order to connect to the servers that house the Colleague Software and associated resources (Informer, WebAdvisor, and UIWeb).

Colleague Access Accounts

This discussion of access accounts is specific to those accounts that are used to access business processes available to users responsible for the execution of business workflows for the college. These types of accounts can only be accessed using the UIWeb interface. Access accounts assigned to individuals for "Self Service" (WebAdvisor) are discussed later.

Before a user can access Colleague processes, they must first have an access account created on the server. Access accounts include the user's login, password, and a list of the Colleague processes that they are authorized to use. User access accounts are created by the MIS Systems

Administrator based on information provided by the user's supervisor AND the Owners or custodians of the processes to be accessed. Users will only be granted access to processes when their supervisor certifies that the access is required to satisfy a job requirement or duty, AND when the owner of the process authorizes this user to access the process. The Systems Administrator will make NO attempt to validate job duties or claims by supervisors when processing requests other than to confirm that the correct owner and supervisor have approved the access.

The college has a formal procedure for submitting written requests for new access accounts and maintenance of existing accounts. Each owner and their designees have access to software designed to assist them with the creation of "Request Forms" that are submitted to MIS for this purpose.   Owner and supervisor signatures on these forms are used by MIS to confirm that the access has been approved by the correct areas. MIS will not create an access account if the request forms are missing signatures, or have been signed by the wrong owner or supervisor.

All approved Request Forms submitted to MIS will be kept on file as required by the Office of the State Auditor.   During each FTE, Financial, and IT audit, the auditors will review a specific set of the Request Forms for users based on the area of the college being audited. When asked to explain or justify a user's access, the MIS position in EVERY case will be that the account was created based on the approval of the owner and supervisor that signed the request, and will direct the auditors to those individuals for justification.

Once an access account has been created for a user, that user is responsible for maintaining the security of their id and password, and must take all reasonable precautions to prevent others from being able to use their account. Login IDs and passwords are not to be shared. As published in the Statewide Security Manual (Standard 020106), passwords shall not be revealed to anyone, including supervisors, co-workers, and family members.

Logging in using the access account

Chapter 2 described the each of the "system layers" that a user must interact with in order to access a Colleague process.   Each user's access account includes the parameters necessary to automatically pass through each of those layers until they see the processes that they are authorized to use. When a user logs using their access account, the operating system layer will validate their login and password. If the login and password are valid, the operating system will then check the password age, and if it is more than 30 days old and less than 60 days old, the user will be required to change it. Once the operating system has validated the password and determined that it is current, the user account and access is passed to the database and Colleague layers.

Once control is passed to the database and Colleague layers, the account information will be used to identify the processes that this user is authorized to access, and presented in a web page format (described in detail later). From that point forward, all user interaction will be with the Colleague processes. Interaction with the database will not be visible to the users, as it is handled by the Colleague processes.

Users are not allowed to have direct access to the database layer. There is very little security at this layer, and the basic assumption is that it is intended for technical staff only. There will be occasions when users are instructed by outside agencies (NCCCS, Ellucian) to perform maintenance tasks, file transfers, or other processes that can only be executed at the database layer, more commonly referred to as the “colon prompt” or “command line”. The System Administrator will execute these processes for them when this happens.

Security at the Colleague layer is handled by processes that run in each of the five Application areas, using process information stored in the access accounts to determine what each user is authorized to do. As describe earlier, the “process information” was provided by the user’s supervisor and the process owners.

Each user’s access account is made up of an operator record and a staff record, and both are stored in the database by the Colleague security processes. These records define who the user is, where they work, their login id, and most importantly security information that can be used to determine what processes they are allowed to access in Colleague. The user accounts do not identify the actual names of processes that the user can access. Instead, the user accounts include the names of Security Classes, which are used to identify groups of processes. An example of a security class might be a class named “ST.REG” that includes all the processes associated the registering students.

A security class is a collection of menus and processes (mnemonics) that have been grouped together based on the following:

- Represent a set of menus, processes or mnemonics required to accomplish a business process, such as all the mnemonics required to enter and validate a student application and related data.

- Represent a set of modules, menus, or processes required to satisfy a job function, such as all the mnemonics required by the Registrar.

The owners and their custodians are responsible for the creation and maintenance of the security classes that control access to the processes that they own. Security Class creation and maintenance requests must be submitted to the MIS Systems Administrator, using the appropriate forms. These forms must be signed by the appropriate Owner or designee before they are processed, and will remain on file in MIS as required by the Office of the State Auditors. Once security classes are created, they can be assigned to users to control their access of processes. Users must have at least one security class assigned to them.

Once the login process has completed the analysis of the user’s access account to identify what processes are available to this user, control is passed to the Colleague application and user until the user chooses to end the session. During the session, the user will only be able to interact with the processes they have been authorized to access. The following is a summary of the login process just described.

1. The user connects to the URL assigned to the Production, Test, or Test2 environment (that they wish to use, and completes the login and password prompts.

2. The UIWeb process connects to the Server and presents the login and password to the Operating System for authentication.

3. The operating system evaluates the age of the password, and if it is older than 30 days the user will be required to select a new password.

4. Once authenticated to the operating system, UI switches to the database environment (Production, Test or Test2) based on the URL connected to.

5. The Colleague application will read the operator and staff records assigned to this user, and will use the security classes to identify what this user is authorized to access.

6. The Colleague application will build a menu tree for the user using the list of authorized processes, present it and relinquish control to the user until they end the session.

More about security classes

Security classes are used to control access of groups of processes. As mentioned earlier, every user's access account will have an operator and staff record, but those records alone will not control the access to processes. In fact, a user that has a properly setup operator and staff record with no security classes assigned to them will have access to every process of every module of every application in the Colleague system.

Owners and custodians must decide what criteria to use when grouping processes into classes. Grouping criteria usually falls into one of two categories, those being to group a set of processes required to accomplish a specific task or function, OR to group a set up processes required by a specific role or job position at the college. These two approaches are referred to as process-based and role-based security.

An example of a process-based security class might be one that groups the processes that are used to cash receipt student tuition payments. Cash receipting is just one of the many functions performed by the Accounts Technicians in Accounts Receivable. Each of these technicians will have this class assigned to them to allow access to the cashiering processes. They will also have additional classes assigned to them to support their other duties. If additional users are ever needed to assist as cashiers during peak registration periods, this class can be assigned and removed after registration, allowing non accounts receivable staff to access the cashiering processes in AR without giving them access to all of the AR processes. Because each function or process for a given area is in a separate class, the owner has more flexibility when it comes to reassigning duties in response to changing business workflows and cycles. Process-based security usually implies that users will have multiple small (few processes) security classes assigned to them.

Using the same scenario, an example of role-based security would be a security class that has been designed to identify every process required by an Account Technician in Accounts Receivable department, not just the cash receipting processes, based on the overall job description. If every technician in the department has identical job duties, then a single class can be created to define the processes required for this job title and assigned to each of them. Role based security is usually fairly easy to setup and maintain, as long as the duties assigned to each individual remain the same. If the duties for one of the individuals with this class change, a new security class will need to be created that includes the changes will have to be created and assigned to those individuals with the changed duties. Role-based security is not as flexible as process-based security in areas where duties and responsibilities may vary, and usually implies that users will have one large security class assigned to them.

Owners and custodians must consider both approaches when deciding how to group processes, using job responsibilities and duties as the basis. The colleague application is made up of thousands of processes. Processes can be named in more than one class, and users can have more than one class assigned to them. The use of security classes supports the idea that there are groups of users that perform similar or identical job functions, and therefore have a need to access similar or identical processes. You can create one security class that defines many processes, or many classes that each defines a set of processes required to perform a single business function.   Once a class is built, it can be assigned to any number of users, and a user can have more than one security class assigned to them.   When multiple classes are assigned, access is based on the combined list of processes.

There are advantages and disadvantages to both process-based and role-based security, and in most cases a combination of both will most likely be deployed. Issues to consider:

- Using role-based security can be very simple to setup as it requires that only a few security classes be built, however each class could potentially have hundreds of processes named in each.
- Using role-based classes to define all of the access for a specific job works perfectly in environments where each user has identical job duties that rarely change. A perfect example would be the access requirements for faculty.
- Role-based classes work well when created to define broader areas of access for supervisors or technical leads in areas. Broader does not imply all of the processes of associated with an Application, such as Student Records or Colleague Financials.   An example might be a class that includes every payroll process so that it can be assigned to the Payroll Supervisor.
- Using Process-based classes requires that each owner or custodian define each of the business functions for their area and identify the processes required to perform that function. Because of this, process-based is harder to setup, but is usually more flexible and easy to maintain than role-based.
- Process-based security is very flexible and creates an environment where owners can easily respond to increased demand for certain business functions. Limited additional processing can be added to a user based on the processes defined in the class.
- Process-based security allows the college to address some functions on a global basis, such as a security class to maintain person demographics that is shared by all areas of the college. Other areas would be Communications Management, Rules Processing, and File uploading and downloading.
- A combination of both types will most likely be the best fit where a role-based class will be used to define all of the requirements of a department supervisor, while process-based classes are defined for each of the functions assigned to the users that work in the department.

Security classes and “Do only, Never do, Inquiry Only, Privileged”

In addition to identifying what processes can be accessed, security classes also identify how each mnemonic can be used, relative to this class assignment only. This is referred to by Colleague as the “access type”. A process can exist in several classes with different access types assigned. For example, a security class can define the process to access name and address data with an access type of read only, while another class defines that same process with full access. The access type of read only will only apply to those users that have that class assigned to them. Each of the access types available is described below:

The “Do Only” type is used to grant access to processes or mnemonics. The name “Do Only” can be misleading, as it is the access type assigned to every process in a security class. The system treats “Do Only” as a cumulative type. If a security class has 30 processes, and each is assigned “Do Only”, the class is granting access to “Do only” those 30 processes. If a user has multiple classes assigned and each class includes processes with “Do Only” access, the lists are combined and treated just like they would if all were named in a single class. If “Do Only” access is granted to a process, and that process calls or drills to other processes, the user will have access to those called processes, with “Do Only” access, whether the process is named in the class or not. For example, if a user has been assigned a class that grants “Do Only” access to NAE, the user will automatically have “Do Only” access to the BIO and DADD processes because they can be called from NAE. This capability can be restricted using the “Never Do” access type described below.

The “Never Do” type is used to explicitly deny access to each process or mnemonic named in the class with this access. This type is beneficial when granting access to processes that can drill to other mnemonics. The “Do only” access can be assigned to grant access to a mnemonic, while restricting the mnemonics that it can drill to by using the “Never Do” access, as described in the in the previous example.

The “Inquiry Only” type is used to limit the capabilities of a process in a class to read only. When a user accesses a process with read only capabilities, they cannot “save” records. To assign

“Inquiry Only” to a process in a class, it must be included in the class as “Do Only”. In other words, access is granted to the process first and then the update capability is removed.

The “Privileged” type is used to control access to the more powerful processes that are used to setup and manage the modules and applications. When this type of access is assigned to a process in a security class, that process cannot be accessed by any user until that same mnemonic is added to another security class as “Do Only” or “Inquiry Only” and both classes are assigned to the users approved to access it. The first security class that defines the process as privileged locks the mnemonic from ALL users, whether it is assigned to them or not. The second class unlocks the process and grants “Do Only” or “Inquiry Only” access to it. If a process is assigned to a security class as privileged, and never assigned to another class, that process will not be available to any user other than the Systems Administrator.

How Security classes are used during login

Each time a user logs into Colleague, an initialization process in the Colleague application will execute the following steps to build a list of processes that the user can access:

1. Creates a master list of every process in the Colleague system.

2. Reads each of the Security classes assigned to the user and compiles a list of each process requested along with the requested access type.

3. Removes all processes from the master list that have not been requested as “Do Only”.

4. Remove all processes from the master list that have been requested as “Never Do”.

5. Changes all processes in the master list that have been requested with access type of “Inquiry Only” so that the update capability is disabled.

6. Confirms that all Privileged processes have been requested with access type of “privileged”. Privileged processes not requested as “privileged” are removed from the master list.

7. The master list is presented to the user as a menu tree, and the Apps menu is set to only allow access to required applications.

Usage tips

If multiple security classes have been assigned to a user and the same process is included in more than one class, the most restrictive access type for that mnemonic will be applied. For example, a user has been setup with 5 security classes assigned to their account, and each class names NAE with “Do Only” access. However, one of the 5 classes also has the “Inquiry Only” access assigned to NAE. This will result in the user having “Inquiry only” access.

The security classes that identify privileged mnemonics will have a global impact on the system regardless of whether they are assigned to users or not. The scope of all other classes will be limited to how it impacts each user that it is assigned to when they login. If these types of classes are not assigned to users, they will have no bearing on the system.

The college has also created security classes that are empty and are used to document access to coupled applications. The classes do not grant access to Colleague processes, but instead, identify by their assigned name and description access to external applications such as the Informer reporting tool. By assigning a class like this to a user, owners can set a reminder for themselves and the System Administrator that in addition to Ellucian access, this user has an account or access on one of the systems coupled to the Ellucian system. For example, a class named UT.INFORMER.CF.PU has been created to identify Informer users that have access to Purchasing data. This class is empty (no mnemonics), however when assigned to users, the Data/Application Owners and System Administrators are aware of the external access.

Access accounts for Self-Service Access

Discussion to this point has focused on the use of access accounts that are created for users that have specific job duties that require that access. Those access accounts are used by employees of the college to satisfy business requirements.

There are also accounts that are created for self-service access. These accounts are used with WebAdvisor, and users are limited to accessing information about themselves. An example would be those processes used by employees to view their pay advices or W2 statements.

Self-service accounts are automatically created by the system for each staff and faculty member based on status information entered by Human Resources when they are hired. Every self-service account used by employees is setup using a standard template, and the capabilities of each account are identical. These accounts utilize a role-based security class that is assigned to all employees. This class defines the self-service processes that are available to all employees.

The owners and custodians need to be aware that these accounts exist, and that they are automatically created when new employees are added to the system.

Chapter 5 Patch and Release Management

The Ellucian Colleague Software is made up of thousands of programs, menus, subroutines, control files, and dictionaries. Each of these items was designed to satisfy specific business requirements, utilizing current technology as it existed when it was developed. As newer technologies emerge, customer expectations expand, and industry requirements change, Ellucian must respond by constantly enhancing Colleague. Typically, enhancements are made and released at regular intervals (weekly), addressing small groups of related processes and components. These types of enhancements, or patches, can be loaded during off hours with very little impact on system availability. Massive changes to Colleague to support migration to newer technologies are delivered in the form of new versions or releases of the product, and require a few days of down time to implement.

When Ellucian enhances Colleague, the changes are released as patches to their customers. The term released in this case simply means that the patch is available for retrieval by customers. It is up to each college that uses Colleague to monitor patch announcements from Ellucian. Announcements will usually include enough information for colleges to determine whether the patch applies to them, the risk or business impact if loaded/not loaded, hardware or operating system dependencies, or dependencies on other patches. Once it has been decided that a patch is needed, the associated risks are acceptable, and dependency requirements met, the College can retrieve the patch and load it into their test environments where owners can test the enhancements. The patch will be loaded into production once the owner has communicated that the patch has been approved for load.

This entire process, from patch announcement to patch implementation, is commonly referred to as Patch Management. The process should be well documented and followed on a consistent basis by colleges to ensure that the Colleague software is kept up to date and secure, AND more importantly to ensure that the college is not taking unnecessary risks. Many colleges include patch management with their overall Change Management procedures and policies. The Statewide Information Security Manual addresses many of the standards associated with the delivery of new software and maintenance of existing software in Chapter 8. Section 080205 specifically addresses “Managing Change control Procedures”.

While this discussion has been focused on the delivery of patches from Ellucian, patches can also be created by the college’s programming staff. Those patches are intended to address items specific to FTCC business requirements. Local patches are not specifically mentioned in this document, however they are handled the same way as patches delivered by Ellucian. The source of the patch is irrelevant to the Patch Management process.

What are the Risks

Ellucian will release changes to Colleague as patches. Patches are bundles of items, and include changes to existing programs, replacement programs, or completely new processes or applications. Ellucian attempts to deliver patches that will not impact the college’s ability to conduct business; however it is impossible for them to test every patch for all of the varying types of environments that might exist at every college. Once the college loads the patch for testing, there is no guarantee that the local testing will reveal any outstanding issues, especially if the patch corrects one issue, but causes a new issue with a related process. The risk of loading each patch should be assessed to determine:

- What impact might this patch have on current workflows and business cycles? For example, the risks of loading payroll patches in the middle of a payroll run.

- What risks is the college taking by not having the latest version of the software. For example, running registration with the current tuition rate tables.

Patch Delivery and the North Carolina Community College System Office.

In the process flow described above, Colleague patches are retrieved directly from Ellucian, and loaded by the colleges. This is not the process for NC Community Colleges.

The version of Colleague software used by the college was created specifically for the North Carolina Community colleges. This version or template is referred to as the North Carolina template, and includes the base Colleague application along with additions and changes that were implemented and maintained by the NC Community College System Office (NCCCSO). Because of this, the college cannot load patches released by Ellucian, as the Ellucian patches are developed for the standard version of the software. Instead, the NCCCSO must load each Ellucian patch into the NC template to determine what impact if any it might have on the customizations made by the system office. Once the NCCCSO has and approved the patch, it will be released to the colleges. If the Ellucian patch impacted the NC Template, additional patches will be released with the Ellucian patch to "undo" any damage to the template. The college will NOT load patches released from Ellucian until they are released by the NCCCSO.

Local Patch Management process

The implementation of Patches and Releases requires a coordinated effort between the Application/Data Owners and the MIS Systems Administrator. That coordinated effort, or Patch Management process, identifies the Application/Data owners as the group responsible for the authorization of loading patches into the Production or Live environment.

The Office of the State Auditors now includes a review of the college's patch management process to insure that it is driven by the process owners instead of MIS. During the last Financials Audit, the auditor presented MIS with a list of patches and requested proof of owner approval prior to loading. The NCCCS office also released the following statement, which was extracted from the NCCCS "Software Update Process" manual.

"SOFTWARE UPDATES USING SAVALET "

"Before any software update from the System Office is moved into the Live Account, there must be some general agreement with the user that the software update has been tested and is ready. It is sometimes difficult to determine what information and documentation the User needs to have so that he can make an informed decision about the need for testing. Colleague is an end user

system, and the users, must take responsibility for testing. No software update should be loaded into the production environment until the department head or some other authority has given approval. "

Patch Flow

The NCCCSO will announce the availability of patches weekly. Announcements are usually emails that are sent to the Systems Administrator on Thursday afternoons. The email does not include the actual patch or documentation, as it is only intended to announce patch availability.

Sample Patch release email announcement

From:	CIS Release Management CIS Release Management
To:	CC CIS Patch
Date:	2/12/2009 2:42 PM
Subject:	Release Package R18_0081

The following list is a release of R18 updates. These updates are retrievable using your school Ellucian ID from the System Office CISPR.

#10467 - N99_XSU200281-R18*001 - Ellucian Software Update (non-impact)
SU41349.59-485*04 - EDX Trigger Condition Enhancements

#10468 - N99_XSU200319-R18*001 - Ellucian Software Update
SU40697.63-1805*03 2008 NSC Maintenance

Release Notes are posted at the secured CIS Documentation area on the System Office web site at:
http://www.nccommunitycolleges.edu/CIS_Docs/patches_R18/templateR18PatchReleases.htm
An Administrator needing the ID and password to the documentation site should contact his or her project manager.

CIS Release Management
CIS_Release_Management@nccommunitycolleges.edu
NC Community College System Office
E-mail correspondence to and from this sender may be subject to the North Carolina Public Records Law and may be disclosed to third parties.

The email includes a URL that points to the location where the release notes are available for download. The System Administrator will download and distribute the release notes via email to the appropriate owners and custodians after the patches are loaded into the test environment.

In addition to the patch announcement, a second email will usually follow that includes a “Forward Schedule of Changes”. This is a spreadsheet that identifies the anticipated release dates of patches that the system office is currently working on. The System Administrator will forward a copy of this spreadsheet to each of the owners and custodians.

The System Administrator will begin the patch load process on either Thursday afternoon or Friday morning by downloading the announced patches and installing them into the Test environment. The System Administrator will then evaluate each patch to determine what owner or area will be impacted by the patch, and emails the patch documentation to those owners. The body of the email (sample on next page) will include specific instructions that explain what the recipient is required to do before the patch will be loaded into the production environment. Attached to the email will be all of the documentation that was included with the patch.

As indicated in the body of the email, each owner has 3 options regarding the review and approval of patches. It is understood that there will be cases where processes that have been patched cannot be tested, or that even if a test can be performed there is no guarantee that the process will run correctly after the patch is applied to the production account. When an owner responds to the System Administrator that a patch has been approved for load, it means that the owner or custodians:

- Have assessed the risk of changing the process in production during the current business cycle.

- Are aware that a process that they own has been changed and that change could impact their business workflows.

- Have notified appropriate stewards in their areas of the changes.

- Have (when possible) tested the changed process in the Test environment.

- Updated internal documentation and manuals to reflect changes.

When an owner responds to the System Administrator that the patch has no impact, they are stating that the process being changed is not being used by the college, such as the Canadian Tax table patches.

When an owner or custodian responds to the System Administrator that the patch does not apply, they are stating that they do not own the process being changed.

Sample Local Patch announcement

From: [redacted]
To: [redacted]
Date: 2/13/2009 4:48 PM
Subject: Patch loaded SU40697 63 1805 03
Attachments: SU40697 63 1805 03.rtf

Attached is documentation describing a new Ellucian patch that has been installed in Test. Please share this documentation with the appropriate personnel in your area to determine what impact this software change might have. This patch will not be loaded into Production without your approval.
To approve the load, reply to this email with the statement “APPROVED for Load” as the message text. Also include your GroupWise signature when you send the reply.
If this patch applies to a function or process not utilized by the college, please reply to this message with the statement “NO IMPACT” as the message text. If this patch does not apply to your area, please reply to this message with the statement “DOES NOT APPLY” as the message text. Also include your GroupWise signature when you send the reply.
Thanks,
[redacted], MIS Systems Administrator

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

As mentioned earlier, the release notes for each patch will be attached to this email as a text or .rtf type file, and can be opened with Microsoft Word, WordPad, Notepad, etc.

Every patch announcement sent to the owners and custodians must be replied to, with one of the three options clearly indicated in the message text section of the email. When replying, always include the message text received in the reply, and confirm that the patch identifier is included in the subject line.   Every email must also include the electronic signature to confirm that the reply is coming from a valid Data/Application owner or Custodian. All replies are filed in the MIS department and will be subject to review by the NC Auditors office.

Patches will not be loaded into the production environment until a response as described above is received. There will be cases where one patch is dependent on other patches. When that occurs, responses for all of the patches with co-dependencies must be received. As a courtesy to other areas of the college, patch announcements should be dealt with as quickly as possible so that this is not a problem.

The patch documentation that accompanies the announcement emails will vary greatly with each patch delivered.   There will be cases when a patch document includes the execution of pre and post installation steps. The System Administrator will be responsible for the steps that require access to the operating system or database command lines. It is assumed that steps involving the execution of application processes or the setting of control parameters are the responsibility of the Data/Application owners and custodians.

All emails, to include the announcements sent to the owners and their replies, are kept on file in MIS for review by the auditors.

Chapter 6 Miscellaneous topics

This chapter will provide additional or related information for some of the topics already covered in previous chapters. Most of the information has been presented with the basic assumption that there is a consistent level of system usage and security awareness across the campus. This may not be the case when applied to some of the specialized areas of the college.

Published College Procedures and Plans

As mentioned in chapter 1, many of the duties and responsibilities of the Data/Application owners extend far beyond the supervision of Colleague usage in their areas. Owners are responsible for ensuring the protection and use of the college's data and processes, whether it is processes and data included in the Ellucian system, standalone workstation applications, or slips of paper used to collect and distribute handwritten information between departments. The college's Administrative Procedures Manual includes the guidelines, standards and procedures that are to be used to accomplish this. It is up to the managers in each area of the college to ensure that their employees are aware of and understand these published procedures, and that their departments operate by those procedures. One particular item in the Administrative Procedures Manual is section I-23.10 (Management Information Services Acceptable Use guidelines). It covers the use of all college technology resources, not just the Ellucian System. This document is revised on a regular basis as newer technologies are implemented by the college. It is also reviewed by the Office of the State Auditors, and is a requirement for PCI compliance (Payment Card Industry).

Another important document is the Colleges Continuity of Operations Plan (COOP) and associated internal unit plans for each department. Owners must ensure that each department in their area has an up to date plan for continuing business activities immediately following a disaster or event that disables their ability to conduct business as they normally would. Each department should consider conducting a risk assessment and mitigation plan to identify the types of risks that exist and how to mitigate impact or damages. Keep in mind, from an Information standpoint, any event that could cause a disruption in business activities is a risk, whether it is a Tornado, Computer Virus, theft, or human error.

The administrative procedures manual and COOP plan can be found on the document list at http://www.faytechcc.edu/inst_effect/Handbooks_Manuals.asp. Yearly (in July), a current copy of individual internal unit plans should be sent to the Director of MIS to be put on file. Additionally, hard copies and electronic copies should be kept within the individual departments for reference in the event of a disaster.

Ensuring the protection and usage of the college's data and processes is the duty of every employee, regardless of whether they own or interact with any of the data or processes. Physical security, such as unlocked doors, unattended offices, misuse of electrical resources or environmental controls all pose as risks that could prevent the college from ensuring that protection. Lack of adequate training, undocumented workflows, and outdated operational procedures will lead to human error, and that will also prevent the college from ensuring that data is protected. A perfect example would be the incorrect running of a Purge process that results in the deletion of 5000 student records instead of the intended 50.

In response to recent audits and Payment Card Industry requirements, the MIS department will conduct this IT Governance training session on an annual basis, limited to the contents of this document. This document will be maintained by MIS to include any new topics as required by the college. This training will be delivered to the Data/Application owners, custodians and stewards. Prior to this training each year, the MIS department will conduct an internal audit of all users and their access rights. Following the internal audit, the data owners will be required to re-certify each user of processes and data that they own. The next internal audits will begin in January 2014. The remainder of this chapter will provide additional information and tools to support some of the duties and responsibilities of the owners.

On Going Training and support resources

Training of operational staff is the responsibility of the Data/Application Owners. Most offices utilize existing custodians and stewards to handle training of new staff and refresher training for existing staff. In addition to internal training, the NCCCSO also offers a full slate of on Going Training to support the colleges with this effort. A full calendar is scheduled training is available at the system office web site:
http://www.nccommunitycolleges.edu/Training/CIS_Training/CISTrainingHomePage.html
From this page, users can search the calendar for course offerings, review course agendas and outlines, register for courses, and download training materials for current courses or archived materials from previous courses. The download of training materials may require a login and password, which can be obtained by contacting the MIS Systems Administrator. Download of training materials should be limited to those individuals responsible for the delivery of training to end users.

In addition to the NCCCSO Training web site are the Ellucian Support and Discussion/Forum pages. Both are available by connecting to www.Ellucian.com, and require a login and password. The Ellucian support page includes access to the AnswerNet resource, where users can search the Ellucian database that stores information about known bugs, patch announcements and workarounds. There is also a documentation download resource that includes all of the Ellucian documentation. Caution must be used when using the AnswerNet information and documentation from this site, as it is specific to the standard version of software released by Ellucian and does not consider the NC template.

The Ellucian discussion/forum is a site where all Ellucian customers can share information, post questions, and search through archives of previous discussions.

NCCCSO Help Desk

The NCCCSO operates a multi-tiered help desk that has been designed to quickly respond to Ellucian issues reported by the colleges. The help desk can be reached by sending an email to

"CIS Help Desk@nccommunitycolleges.edu" or by phone at 919-807-7048. If the help desk is called, follow-up email will be required to provide additional information requested. When emailing the help desk, provide as much information about the issue as possible, to include all captured screen shots and error messages. Also indicate which of the following priority codes best matches the impact of the issue being reported and a desired resolution completion date.
Emergency The problem impedes your ability to function, and there is no work around. Must be resolved in three days or less.

- Urgent - Problem impedes your ability to function, and an unacceptable work around exists. The incident will become an Emergency in the next 30 days if not resolved.
- High - Problem impedes your ability to function; however, a reasonable workaround exists. The objective is to develop and implement a permanent solution for the workaround by the date specified in the impact statement.
- Medium - Problem impairs an application's functionality but does not prevent work from being done. The objective is to develop a resolution for the impaired functionality by the date specified in the impact statement. Resolution may include designating the incident as an item for future enhancement to the College Information System (CIS).
- Low - An Incident Report that is defined as NC Template inquiries or modifications that do not impair the application's functionality or the ability to do work. The objective is to develop a resolution or answer the question by the date specified in the impact statement. Resolution may include designating the incident as an item for future enhancement to the CIS.

Once the help desk has received the call or email, a Help Desk Ticket (HDT) will be opened and the person submitting the issue will be notified by email. This HDT will have a unique identifier assigned to it that should be used for all reference and dialog until the problem is resolved.

NCCSO Subject Matter Experts

The following lists identify the Subject Matter Experts provided by the NCCCSO. There are 2 experts listed for each subject, one for each region listed. The second list identifies what region each college is in. FTCC is required to contact the east region experts, however when working with other colleges on a particular problem or issue, it will be beneficial to know what region they are in and who the subject matter expert might be.

Subject Matter Experts as of May 13, 2013

Position	Name	State Region	College Location	Contact Information
SME - Continuing Education	[redacted]	East	System Office	~~919-807-7189~~ ~~masseyr@nccommunitycolleges.edu~~
SME - Continuing Education	[redacted]	West	Mitchell CC	~~704-978-5433~~
SME - Curriculum	[redacted]	East	Pitt CC	~~252-493-7255~~ ~~bartleys@nccommunitycolleges.edu~~
SME - Curriculum	[redacted]	West	Tri-County CC	~~828-835-4228~~ ~~rickettj@nccommunitycolleges.edu~~
SME - Financial Aid	[redacted]	East	Johnston CC	~~919-209-2181~~ ~~statlerk@nccommunitycolleges.edu~~
SME - Financial Aid	[redacted]	West	TBD	~~TBD~~
SME - Human Resources/Payroll	[redacted]	West	Guilford TCC	~~336-334-4822 Ext. 50376~~ ~~millerm@nccommunitycolleges.edu~~
SME - Human Resources/Payroll	[redacted]	East	TBD	~~TBD~~
SME - Technical	[redacted]	East/West	System Office	~~919-807-7174~~ ~~boyetted@nccommunitycolleges.edu~~
SME - College Financials	[redacted]	West	Montgomery CC	~~910-576-6222 Ext. 531~~ ~~martinh@nccommunitycolleges.edu~~
SME - College Financials	[redacted]	East	Johnston CC	~~919-209-2571~~ ~~battend@nccommunitycolleges.edu~~
SME - College Financials (E-Procurement, Fixed Assets, Accounts Payable, Purchasing)	[redacted]	East/West	System Office	~~919-807-7035~~ ~~danielsc@nccommunitycolleges.edu~~

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted Table

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Test Environments Refresh

As described in chapter 2, the Ellucian software application and associated data is available in 4 different environments on the system. The Production environment includes the version of all software approved for use by the owners, and the most current version of all college data. The Test and Test2 environments include the last version of software released to the college, and a dated copy of all data from the production account. The test environments are an excellent area for departments to train new employees, test patches, and experiment with a process that they are not familiar with, without risking the integrity of the college's production data. The Test environment includes a test instance of WebAdvisor to provide a web application test environment in addition to the testing of UI accessible applications. The Test2 environment is limited to UI access only.

After a period of time, the Test environments will lose their testing effectiveness due to the age of the data. When this occurs, the data in either or both test environments can be refreshed from the data in the production environment. When this refresh is run, it will replace all of the data in the test environment being refreshed. The refresh of an environment cannot be limited to only refresh data for a specific module or application. Because of this, refreshes must be coordinated between the owners and MIS to avoid destroying an existing test being executed by a department. Refreshes can take up to 2 hours per environment to complete, and require that no users be logged into the environment during the refresh.

Refreshes must be requested in writing a minimum of 2 days prior to execution for planning and coordination. It will be assumed that the owner or custodian submitting the requested has gotten approval from all areas of the college that will be impacted.

Appendices follow this page.

Appendix A - Statewide Information Security Manual – Introduction and Guidance

Introduction for Information Security Manual

The Information Security Manual is the foundation for information technology security in North Carolina Community Colleges. It is used to establish a set of standards for information technology security to maximize the functionality, security, and interoperability of the Colleges' distributed information technology assets.

The Manual is based on industry best practices and follows the International Organization for Standardization Standard 27002 (ISO 27002) for information technology security framework, and incorporates references to the National Institute of Standards and Technology (NIST) and other relevant standards. These security standards have been extensively reviewed by representatives of the North Carolina Community Colleges.

The Information Security Manual sets forth the basic information technology security requirements for the College. Standing alone, it provides each College with a basic information security manual. Some Colleges may need to supplement the manual with more detailed policies and standards that relate to their operations and any applicable statutory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Internal Revenue Code.

Guidance for Colleges

While this Manual is based on the foundation of the State of North Carolina Information Security Manual simply adopting these standards will not provide a comprehensive security program. College management should emphasize the importance of information security throughout their institution with applicable College specific security policies, ongoing training and sufficient personnel, resources and support.   When considering the specific controls that are to be used to comply with the security standards, Colleges should refer to the security practices related to information technology implementation as described in the NC Statewide Technical Architecture. The architecture is the means by which College's achieve compliance to the statewide information security standards. Colleges opting to deviate from these standards may be required to provide justification to explain any deviation.

These standards should be followed by College personnel and their computing devices used for administrative computing purposes. It is noted that individual Colleges are academic institutions and classroom instruction (especially in Information Technology curriculums) may be hindered if all standards in this manual are followed. Therefore, classroom computing devices used for instructional purposes (*i.e.,* instructional labs, classroom computers, classroom instructor workstations, presenter workstations) may be exempt from certain standards and guidelines defined in this manual. These standards, as outlined in this manual, are to be subject to the individual College's instructional needs and requirements.

Implementation and Management

College administration should also consider periodic internal and external reviews of their information security program. The reviews may be staggered but should collectively include technical security controls, such as devices and networks, and non-technical security controls, which include policies, processes, and self-reviews. Independent information security reviews should also be considered when there are significant changes to the College information security posture because of a technology overhaul, significant change in business case or information protection needs.

ISO 27002 REFERENCES

6.1.1 Management commitment to information security

6.1.2 Information security coordination

6.1.3 Allocation of information security responsibilities
6.1.8 Independent review of information security

Chapter 1 – Classifying Information and Data

Section 01 Setting Classification Standards

010101 Defining Information

Purpose: To protect the College’s information.

STANDARD

Information includes all data, regardless of physical form or characteristics, made or received in connection with the transaction of public business by any College or State government.

The College’s information shall be handled in a manner that protects the information from unauthorized or accidental disclosure, modification or loss. All Colleges shall maintain a comprehensive and up-to-date database of their information assets and periodically review the database to ensure that it is complete and accurate.

Each College, through its management, is required to protect and secure the information assets under its control. The basic information requirements include, but are not limited to:

- Identifying information assets and maintaining a current inventory of information assets.
- Complying with applicable federal and state laws, such as the Family Educational Rights and Privacy Acts (FERPA) and Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- Assessing the vulnerability and risk associated with information assets.
- Determining the value of information assets to the organization and the business processes they support.
- Providing the level of information protection for information assets that is appropriate to their vulnerability, risk level, and organizational value.
- Maintaining a business and disaster recovery plan with respect to information technology and process.

ISO 27002 REFERENCE

7.2.1 Classification guidelines

010102 Labeling Classified Information

Purpose: To protect the College's information through proper classification.

STANDARD

All data shall be labeled to reflect their classification, including their confidentiality, criticality and value to the College and the public. All data must be clearly labeled so that all users are aware of the custodian, classification and value of the data.

ISO 27002 REFERENCE

7.2.2 Information labeling and handling

010103 Storing and Handling Classified Information

Purpose: To protect the College's Information, including information security records, through the establishment of proper controls.

STANDARD

The College's information, data and documents shall be handled in a manner that will protect the information, data and documents from unauthorized or accidental disclosure, modification or loss. All information, data and documents must be processed and stored in accordance with the classification levels assigned to those data in order to protect their integrity, availability and, if applicable, confidentiality.

The type and degree of protection required shall be commensurate with the nature of the information, the operating environment, and the potential exposures resulting from loss, misuse or unauthorized access to or modification of the data.

A College that uses confidential information from another College shall observe and maintain the confidentiality conditions imposed by the providing College if legally possible.[1]

Special protection and handling shall be provided for information that is covered by statutes that address, for example, the confidentiality of financial records, taxpayer information and individual census data.

The State CIO (SCIO) shall manage and protect confidential information technology security records that Colleges provide to SCIO's office and the Office of Information Technology Services (ITS). The records submitted to the State CIO or ITS that are confidential because the records disclose information technology security features shall so designate the records by affixing the following statement, "Confidential per G.S. §132-6.1(c)", on each page.

Confidential information technology security records shall be provided only to Colleges and their designated representatives when necessary to perform their job functions.

Confidential information technology security records shall not be transmitted electronically over public[2] networks unless encrypted while in transit.[2]

Employees who are provided access to information technology security records shall sign a non-disclosure agreement that includes restrictions on the use and dissemination of the records. Colleges shall ensure that legal and business risks associated with contractors' access are determined, assessed and appropriate measures are taken. Such measures may include, but are not limited to, non-disclosure agreements, contracts, and indemnities.

[1] *See*, News and Observer v. Poole, 330 N.C. 465, 412 S.E.2d 7 (1992).

[2] For the purpose of this standard, a public network includes the State Network. It does not apply to internal College networks which may or may not serve multiple campus locations.

GUIDELINES

- An appropriate set of procedures should be defined for information labelling and handling in accordance with the classification scheme adopted by the College. The procedures should cover information assets in both physical and electronic formats. For each classification, handling procedures should be defined to cover the following types of information-processing activity:
  - Copying
  - Storage
  - Transmission by post, fax, and electronic mail
  - Transmission by spoken word, including mobile phone, voice mail, and answering machines
- Output from systems containing information that is classified as confidential or critical should carry an appropriate classification label. The labelling should reflect the classification according to the rules established by Standard 010102, Setting Classification Standards—Labelling Information. Items for consideration include printed reports, screen displays, recorded media (e.g., tapes, disks, CDs, cassettes, USB flash memory drives), electronic messages and file transfers.
- Where appropriate, physical assets should be labelled. Physical labels are generally the most appropriate forms of labelling. However, some information assets, such as documents in electronic form, cannot be physically labelled and electronic means of labelling need to be used. In other cases, such as with tapes, a physical label is appropriate for the outside of the tape in addition to electronic labelling of documents contained on the tape.
- The originator of a telephone call, a telex/cable, a facsimile transmission, an email, a computer transaction, or any other telecommunications transmission should be aware of the possibility of compromise of confidentiality or integrity of the information transmitted and determine whether the information requires additional special protection and handling.

ISO 27002 REFERENCE

10.7.3 Information handling procedures

010104 *Isolating Top Secret Information*

Purpose: To protect classified federal information.

STANDARD

When Colleges receive information, data or documents classified as Top Secret from the federal government, that information, those data, or those documents shall be stored in a separate secure area and handled as required by federal law.

ISO 27002 REFERENCES

7.2.2 Information labeling and handling

11.6.2 Sensitive system isolation

010105 Classifying Information

Purpose: To protect the College’s information.

STANDARD

All College information and data shall be classified as to its confidentiality, its value and its criticality. Colleges shall establish procedures for evaluating information and data to ensure that they are classified appropriately.

Confidentiality is to be determined in accordance with N.C.G.S. Chapter 132—Public Records Law—and all other applicable legal and regulatory requirements. Data, files, and software shall be marked with a designator that identifies the process by which such information is to be made available or accessible.

ISO 27002 REFERENCE

7.2 Information classification

010106 Accepting Ownership for Classified Information

Purpose: To establish procedures for data handling.

STANDARD

College custodians of data and their designees are responsible for College data and shall establish procedures for appropriate data handling.

ISO 27002 REFERENCES

7.1.1 Inventory of assets

7.1.2 Ownership of assets

7.2 Information classification

010107 Managing Network Security

Purpose: To protect the College’s information through access control procedures.

STANDARD

Network security shall be managed by each College based on business needs and the associated risks.

Access to information available through the State network shall be strictly controlled in accordance with approved access control procedures. Users shall have direct access only to those services that they have been authorized to use.

ISO 27002 REFERENCE
10.6.1 Network controls

Appendix C - Statewide Information Security Manual – Access Standards (from chapter 2)

Section 01 Controlling Access to Information and Systems

020101 Managing Access Control Standards

Purpose: To establish requirements for controlling access to the College's information assets.

STANDARD

Access to College information technology assets shall be controlled and managed to ensure that only authorized devices/persons have access as is appropriate for the College in accordance with the College's business needs.

All computers that are permanently or intermittently connected to internal computer networks shall have an approved password-based access control system. Regardless of the network connections, all computers handling confidential information shall employ approved password-based access control systems. Only authorized users shall be granted access to the College's information systems, and the principle of least privilege shall be used and enforced. Job duties shall be separated as appropriate to prevent any single person or user from having any access not required by their job function.

Access shall be controlled by the following:

- Standard user profiles.
- Documented semi-annual review of users' rights.
- Documented review of privileged accounts every quarter.
- Restriction of connection time.
- Immediate termination of access upon severance or leaving employment.

To ensure that data processed are the actual data required by the data custodian, predetermined times for processing those data must be set by the interested parties to protect the integrity of the data (e.g., preset batch file transmission times).

ISO 27002 REFERENCES

11.1.1 Access control policy

11.2.4 Review of user access rights

11.5.6 Limitation of connection time

020102 Managing User Access

Purpose: To prevent unauthorized access to College networks.

STANDARD

Colleges shall be responsible for establishing a procedure for managing access rights for users of their networks throughout the life cycle of the user ID. Colleges shall identify a backup system administrator to assist with user ID management when the primary system administrator is unavailable.

Only authorized users shall be granted access to College information systems. Users shall be responsible for maintaining the security of their user IDs and passwords. User IDs shall be individually assigned in order to maintain accountability. Each user ID shall be used by only a single individual, who is responsible for every action initiated by the account linked to that user ID. Where supported, the system shall display (after successful login) the date and time of last use of the individual's account so that unauthorized use may be detected.

User IDs shall be disabled promptly upon a user's termination from work for the State or upon cessation of a user's need to access a system or application. User IDs that are inactive for a maximum of 90 days must be disabled, except as specifically exempted by the security administrator. All accounts that have been disabled for greater than 365 days shall be deleted.

Only authorized system or security administrators or an authorized service desk staff shall be allowed to enable or re-enable a user ID except in situations where a user can do so automatically through challenge/response questions or other user self-service mechanisms.

Logging of Administrator Activity

All user ID creation, deletion and change activity performed by system administrators and others with privileged user IDs shall be securely logged and reviewed on a regular basis.

Concurrent Connections

For those systems that enforce a maximum number of concurrent connections for an individual user ID, the number of concurrent connections must be set to two (2).

Outside User IDs

User IDs established for a nonemployee/contractor must have a specified expiration date unless the provision of a user ID without a specified expiration date is approved in writing by the College security liaison. If an expiration date is not provided, a default of thirty (30) days must be used.

Access control may need to be modified in response to the confidentiality of information contained on the system, if existing access controls pose a risk that confidentiality may be breached.

ISO 27002 REFERENCE

11.2 User access management

020103 Securing Unattended Work Stations

Purpose: To prevent unauthorized system access.

STANDARD

Workstations shall be safeguarded from unauthorized access—especially when left unattended. Each College shall be responsible for configuring all workstations to require a password-protected screen saver after a maximum of thirty (30) minutes of inactivity. Users shall not disable the password-protected configuration specifications established by their College. Users should lock their workstations when leaving them unattended.

ISO 27002 REFERENCES

11.3.2 Unattended user equipment

11.3.3 Clear desk and clear screen policy

020105 Controlling Access to Operating System Software

Purpose: To limit access to operating system software to those individuals authorized to perform system administration/management functions.

STANDARD

Only those individuals designated as system administrators shall have access to operating system commands. System administrators shall ensure that all current maintenance and security vulnerability patches are applied and that only essential application ports are opened in the system's firewall.

- Internal network addresses and configuration and other system design information shall be limited to only those individuals who require access in the performance of tasks or services essential to the fulfilment of a work assignment, contract or program.
- State Colleges shall maintain a list of administrative contacts for their systems.
- All authorized users of administrative-access accounts shall have management instructions, documentation and training.
- Each individual who uses an administrative-access account shall use the account only for administrative duties. For other work being performed, the individual shall use a regular user account.
- Each account used for administrative access shall comply with Standard 020106, Managing Passwords.
- When special-access accounts are needed for internal or external audit, software development, software installation, or other defined need, they shall be authorized in advance by management and shall be:
- Created with a specific expiration date.
- Removed when the work is completed.
- Administrative-access accounts must connect in a secure manner at all times.

ISO 27002 REFERENCE

11.5 Operating System Access Control

020108 Restricting Access

Purpose: To ensure that information system access is granted only to authorized users.

STANDARD

Colleges shall establish appropriate controls on access to information systems to allow only those authorized to access the data residing on those systems to do so.

Users of College information systems shall be provided access to information and system functions in accordance with Standard 020101, Managing Access Control Standards.

Access to confidential information shall be restricted to authorized individuals who require access to the information as part of their job responsibilities.

A College may change, restrict or eliminate user access privileges at any time.

ISO 27002 REFERENCE

11.6.1 Information access restriction

020110 Giving Access to Files and Documents

Purpose: To prevent the unauthorized or accidental copying, moving, editing or deleting of data and to protect the confidentiality, integrity and availability of the information assets of North Carolina.

STANDARD

Custodians of data shall assign staff the responsibility for administering and maintaining the rights and permissions for accessing the data and information.

- Users shall be provided with access to information and systems in accordance with a defined standard of access control such as:
- Discretionary access control.
- Mandatory access control.
- Lattice-based access control.
- Rule-based access control.
- Role-based access control.
- Access control lists.
- The default for access is role-based access control for files and documents.
- Access rights of users in the form of read, write and execute shall be controlled appropriately and the outputs of those rights shall be seen only by authorized individuals.
- User rights shall be reviewed at six (6)-month intervals.

- A three (3)-month review cycle shall be required for special access privileges. General user access rights shall be reviewed regularly to ensure that unauthorized privileges have not been obtained.

ISO 27002 REFERENCE

11.2.4 Review of user access rights

020111 Managing Higher Risk System Access

Purpose: To protect the confidentiality, integrity and availability of data on high-risk information technology systems in State government.

STANDARD

Certain systems and applications, because of the nature of the data contained in them, require special management oversight and shall be classified as high-risk. Many times these high-risk systems contain confidential data. At a minimum, these systems shall require access control equal to that specified in Standard 020101, Managing Access Control Standards.

All systems and applications shall be classified through a risk assessment to determine, in part, whether they are high-risk systems.

Guidance

At a minimum, the following should be considered when implementing controls for high-risk systems:

- Whether access to the system is allowed from an external site.
- Hardening of the operating system.
- Criminal Background checks of personnel, vendors and contractors in contact with the system and applications.
- Disaster recovery planning.
- The consequences of loss of data security.

ISO 27002 REFERENCE

11.6.2 Sensitive system isolation

Chapter 11 – Delivering Training and Staff Awareness

Section 01 - Awareness

110101 Delivering Awareness Programs to Permanent Staff

Purpose: To provide awareness programs that ensure employees are familiar with information technology security policies, standards and procedures.

STANDARD

The senior management of each College shall lead by example by ensuring that information security is given a high priority in all current and future activities and initiatives. The College, through senior management, shall provide regular and relevant information security awareness communications to all staff by various means, which include but are not limited to the following:

- Electronic updates, briefings, pamphlets and newsletters.
- Information security awareness tools to enhance awareness and educate staff on information technology security threats and the appropriate safeguards.
- An employee handbook or summary of information security policies, which shall be formally delivered to and signed by employees before they access College resources.

ISO 27002 REFERENCE

8.2.2 Information security awareness, education and training

110102 Third Party Contractor: Awareness Programs

Purpose: To ensure that contractors are familiar with information technology security policies, standards and procedures.

STANDARD

All contractors shall have provisions in their contracts with Colleges that set forth the requirement that they must comply with all College information technology security policies. The College shall provide contractors with regular and relevant information technology security policies. The College shall provide regular and relevant information security awareness communications to contractors by various means, which include but are not limited to the following:

- A handbook or summary of information security policies, which shall be formally delivered to and signed by contractors before they begin work.
- Mandatory information security awareness training before beginning work.
- Formal information technology security training appropriate for work responsibilities, on a regular basis and whenever their work responsibilities change
- Training in information security threats and safeguards, with the extent of technical details to reflect the contractor's individual responsibility for configuring and maintaining information security.

ISO 27002 REFERENCES

6.2.3 Addressing security in third party agreements

8.2.2 Information security awareness, education and training

110103 Delivering Awareness Programs to Temporary Staff

The standard recommended for this section is covered by Standard 110101

110104 *Drafting Top Management Security Communications to Staff*

Purpose: To ensure that top management takes the lead in giving information security a high priority throughout the College.

STANDARD

Senior management within the College shall ensure that information security communications are given priority by staff and shall support information security education programs.

ISO 27002 REFERENCE
5.1.2 Review of the information security policy

110105 Providing Regular Information Updates to Staff

Purpose: To ensure regular and relevant information is passed down to staff from senior management.

STANDARD

Colleges shall provide information relevant to effective information security practices to staff members in a timely manner.

On a periodic basis, senior management shall receive input from information security staff on the effectiveness of the organization's information security measures and recommended improvements.

ISO 27002 REFERENCE

5.1.2 Review of the information security policy

Section 02 - Training

110201 Information Security Training on New Systems

Purpose: To ensure that employees, contractors and temporary employees understand the security implications of new technology.

STANDARD

All users of new systems shall receive training to ensure that their use of the systems is effective and does not compromise information security. Colleges shall train users on how new systems will integrate into their current responsibilities. Colleges shall notify staff of all existing and any new policies that apply to new systems.

ISO 27002 REFERENCE

8.2.2 Information security awareness, education and training

110202 Information Security Officer: Training

Purpose: To ensure that the College information security officer receives adequate training.

STANDARD

The information security officer of each College or his/her equivalent, at a minimum, shall receive annual formalized training on the latest threats to information technology systems and on information security protocols. Senior management shall work with the information security officer on a regular basis to provide the information security officer with knowledge of the College's operational and strategic objectives.

The training for the information security officer must include new technologies to combat threats and updates on new threats to network security and may include updated incident response protocols.

GUIDELINES

Training may be enhanced through:

- Membership in technical societies, clubs, boards, or focus groups.
- Subscriptions to technical documents such as newsletters, magazines and white papers.
- Self-study and certifications relevant to information security.

ISO 27002 REFERENCE

8.2.2 Information security awareness, education and training

110203 User: Information Security Training

Purpose: To ensure that all users receive adequate training.

STANDARD

All Colleges shall provide training to users on relevant information security threats and safeguards. The extent of technical training shall reflect the employee's or contractor's individual responsibility for configuration and/or maintaining information security systems. When staff members change jobs, their information security needs must be reassessed, and any new training on procedures or proper use of information-processing facilities shall be provided as a priority.

College training shall include but not be limited to the following:

- Mandatory information security awareness training before beginning work.
- Formal information technology security training appropriate for work responsibilities, on an annual basis.
- Training in information security threats and safeguards, with the technical details to reflect the employee's or contractor's individual responsibility for configuring and maintaining information security.

ISO 27002 REFERENCE

8.2.2 Information security awareness, education and training

110204 Technical Staff: Information Security Training

Purpose: To ensure that College technical staff receive adequate training.

STANDARD

Colleges shall make specialized training available for technical staff in critical areas of information technology security, including vendor specifically recommended safeguards to improve:

- Server and PC security management.
- Packet-filtering techniques implemented on routers, firewalls, etc.
- Intrusion detection and prevention.
- Software configuration, change and patch management.
- Virus prevention/protection procedures.
- Business continuity practices and procedures.

When staff members who are responsible for information technology systems change jobs, their information security needs must be reassessed, and any new training on procedures or proper use of information-processing facilities shall be provided as a priority.

ISO 27002 REFERENCE

8.2.2 Information security awareness, education and training

110205 Training New Recruits in Information Security

Purpose: To ensure that new employees are aware of good information security practices.

STANDARD

All Colleges shall provide new employees and contractors with mandatory information security training as part of job orientation.

ISO 27002 REFERENCE

8.2.2 Information security awareness, education and training

Chapter 12 – Complying with Legal and Policy Requirements

Section 01 - Complying with Legal Obligations

120101 Being Aware of Legal Obligations

Purpose: To ensure that employees are familiar with the laws that govern use of information technology systems and the data contained within those systems.

STANDARD

Colleges shall ensure that all employees and contractors are aware of legal and regulatory requirements that address the use of information technology systems and the data that reside on those systems.

Colleges also must ensure that each employee and other College Network user is provided with a summary of the legal and regulatory requirements.

Examples of laws that affect computer and telecommunications use in North Carolina are as follows:

- Federal
  - 18 U.S.C. §1030. Fraud and related activity in connection with computers.
  - 17 U.S.C.§§ 500 and 506. Copyright infringements and remedies.
- North Carolina
  - N.C.G.S. §114-15.1. Misuse of state property.
  - N.C.G.S. §14-196. Using profane, indecent or threatening language to any person over the telephone; annoying or harassing by repeated telephoning or making false statements over telephone. The statute includes the sending by computer modem of any false language concerning death, injury, illness, disfigurement, indecent conduct or criminal conduct of the person receiving the information or any close family member.
  - N.C.G.S. §14-454. Accessing computers.
  - N.C.G.S. §14-455. Damaging computers, computer systems, computer networks, and resources.
  - N.C.G.S. §14-457. Extortion.
  - N.C.G.S. §14-458. Computer trespass; penalty.

- N.C.G.S. §14-155. Unauthorized connections with telephone or telegraph.

Examples of laws that affect data residing on State information technology systems are as follows:

- Federal
  - 26 U.S.C. §§6103, 7213, 7213A, 7431, Internal Revenue Code.
  - Public Law 104-191, 104th Congress, Health Insurance Portability and Accountability Act of 1996.
  - 5 U.S.C. §552a, as amended. Privacy Act of 1974.
- North Carolina
  - N.C.G.S. Chapter 132. Public records law.
  - N.C.G.S. §105-259. Secrecy required of officials.
  - N.C.G.S. §122C-52. Client rights to confidentiality.

Laws that relate to confidential records held by North Carolina government are summarized in the following document:

http://www.records.ncdcr.gov/guides/confidential_publicrec_2009.pdf

ISO 27002 References

8.1.3 Terms and conditions of employment

15.1.1 Identification of applicable legislation

120102 Complying with State and Federal Records Laws

Purpose: To ensure that Colleges comply with laws that address proper handling of data contained in information technology systems.

STANDARD

Colleges are subject to State laws governing the use of information technology systems and the data contained in those systems. In some situations, Colleges are also subject to federal laws. Colleges shall take affirmative actions to comply with all applicable laws and take measures to protect the information technology systems and the data contained within information systems.

ISO 27002 References

15.1.4 Data protection and privacy of personal information

120103 Complying with General Copyright Laws

Purpose: To ensure that Colleges comply with laws that address copyright protection.

STANDARD

Colleges shall provide employees with guidelines for obeying software licensing agreements and shall not permit the installation of unauthorized copies of commercial software on technology devices that connect to the State Network.

The guidelines shall inform employees that:

- Persons involved in the illegal reproduction of software can be subject to civil damages and criminal penalties.
- Employees shall obey licensing agreements and shall not install unauthorized copies of commercial software on State College technology devices.
- State employees who make, acquire or use unauthorized copies of computer software shall be disciplined as appropriate. Such discipline may include termination.

ISO 27002 References

15.1.1 Identification of applicable legislation

120104 Complying with Database Copyright Law

Purpose: To ensure that Colleges comply with laws that address copyright protection

STANDARD

Colleges shall inform their employees of any proprietary rights in databases or similar compilations and the appropriate use of such data. Colleges shall also inform employees of any sanctions that may arise from inappropriate use of the databases or similar compilations.

ISO 27002 References

15.1.2 Intellectual property rights (IPR)

120105 Complying with Copyright and Software Licensing Requirements

Purpose: To ensure that Colleges comply with copyright and licensing requirements.

STANDARD

Each College shall establish procedures for software use, distribution and removal within the College to ensure that College use of software meets all copyright and licensing requirements. The procedures shall include the development of internal controls to monitor the number of licenses available and the number of copies in use.

ISO 27002 References

15.1.2 Intellectual property rights (IPR)

120106 Legal Safeguards against Computer Misuse

Purpose: To disclose to users of State information systems the legal policy requirements for using State information technology resources as well as any methods a College may use to monitor usage.

STANDARD

Colleges shall provide users of information technology services with the legal policy requirements that apply to use of State information technology systems and, where practical and appropriate, Colleges shall provide notice to users of State information technology systems that they are using government computer systems.

If Colleges monitor computer users, Colleges also shall provide notice to computer users that their activities on State information technology systems may be monitored and disclosed to third parties.

GUIDELINES

The notice required by this standard can take many forms. An Internet Web page may have a link to a privacy statement. Monitoring notices can consist of stickers pasted to a computer monitor or an electronic notice that displays when the user logs on to a computer. Where practical and appropriate, sign-on warning banners shall be posted on State government computer systems to appear just before or just after login on all systems that are connected to the State Network, giving notice to users that they are accessing State resources and that their actions while they are using these resources may be subject to disclosure to third parties, including law enforcement personnel.

Examples of warning banners:

- WARNING: This is a government computer system, which may be accessed and used only for authorized business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil and/or administrative action.
- All information on this computer system may be intercepted, recorded, read, copied and disclosed by and to authorized personnel for official purposes, including criminal investigations. Such information includes data encrypted to comply with confidentiality and privacy requirements. Access or use of this computer system by any person, whether authorized or unauthorized, constitutes consent to these terms. There is no right of privacy in this system.
- NOTICE: This system is the property of the State of North Carolina and is for authorized use only. Unauthorized access is a violation of federal and State law. All software, data transactions and electronic communications are subject to monitoring.
- This is a government system restricted to authorized use and subject to being monitored at any time. Anyone using this system expressly consents to such monitoring and to any evidence of unauthorized access, use or modification being used for criminal prosecution and civil litigation.
- *Notice to Users.* This is a government computer system and is the property of the State of North Carolina. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.
- Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected and disclosed to law enforcement personnel, as well as to authorized officials of other Colleges. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection and disclosure at the discretion of the agency.
- Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system, you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

ISO 27002 References

15.1.5 Prevention of misuse of information processing facilities

Section 02 - Complying with Policies

120201 Managing Media Storage and Record Retention

Purpose: To establish standard for records retention and disposition.

STANDARD

For the records they create or receive in the course of performing the public's business, Colleges are required to formulate complete and accurate record retention and disposition schedules that comply with the provisions of N.C.G.S. §§121-5 and 132-1, *et seq.* Colleges must manage their records according to the schedules, as approved by the Department of Cultural Resources, State Records Branch, throughout the records' life cycle, from creation to disposition.

ISO 27002 References

15.1.3 Protection of organizational records

120202 Complying with Information Security Standards and Policy

Purpose: To establish security standards and policy compliance requirements for employees.

STANDARD

Colleges shall establish requirements for mandatory compliance with the applicable statewide and individual College information technology security standards and policies. The requirements shall include regular policy and standard reviews for employees and contractors and periodic reviews of information technology systems to determine whether the systems are in compliance with applicable policies and standards.

ISO 27002 References

8.1.3 Terms and conditions of employment

15.2.1 Compliance with security policies and standards

Section 03 - Avoiding Litigation

120302 Using Copyrighted Information from the Internet

Purpose: To comply with applicable copyright laws.

STANDARD

Colleges shall seek legal review before using copyrighted information.

ISO 27002 References

15.1.2 Intellectual property rights (IPR)

120303 Sending Copyrighted Information Electronically

Purpose: To comply with applicable copyright laws.

STANDARD

Colleges shall seek legal review before sending copyrighted information electronically.

ISO 27002 References

15.1.2 Intellectual property rights (IPR)

120304 Using Text directly from Reports, Books or Documents

Purpose: To comply with applicable copyright laws

STANDARD

Colleges shall seek legal review before using copyrighted information contained in reports, books and documents.

ISO 27002 References

15.1.2 Intellectual property rights (IPR)

120305 Infringement of Copyright

Colleges shall define policies and procedures to comply with legal and regulatory requirements in regards to the protection of intellectual property.

GUIDELINES

See Using the Internet for Work Purposes 030312.

ISO 27002 REFERENCES

15.1.2 Intellectual property rights (IPR)

Section 04 - Other Legal Issues

120401 Recording Evidence of Information Security Incidents

Purpose: To create formal records of information technology security incidents.

STANDARD

Colleges shall record information technology security incidents on the Incident Reporting form,[3] incorporated by reference.

Colleges shall also establish formal procedures for recording and retaining evidence relating to information security incidents to ensure that the evidence is properly preserved for any legal actions that may ensue as a result of the incidents.

ISO 27002 References

10.10.1 Audit logging

[3] The Incident Reporting form can be found at https://incident.its.state.nc.us/ and can be filled out online.

10.10.2	Monitoring system use
13.1.1	Reporting information security events
13.2.3	Collection of evidence
15.1	Compliance with legal requirements