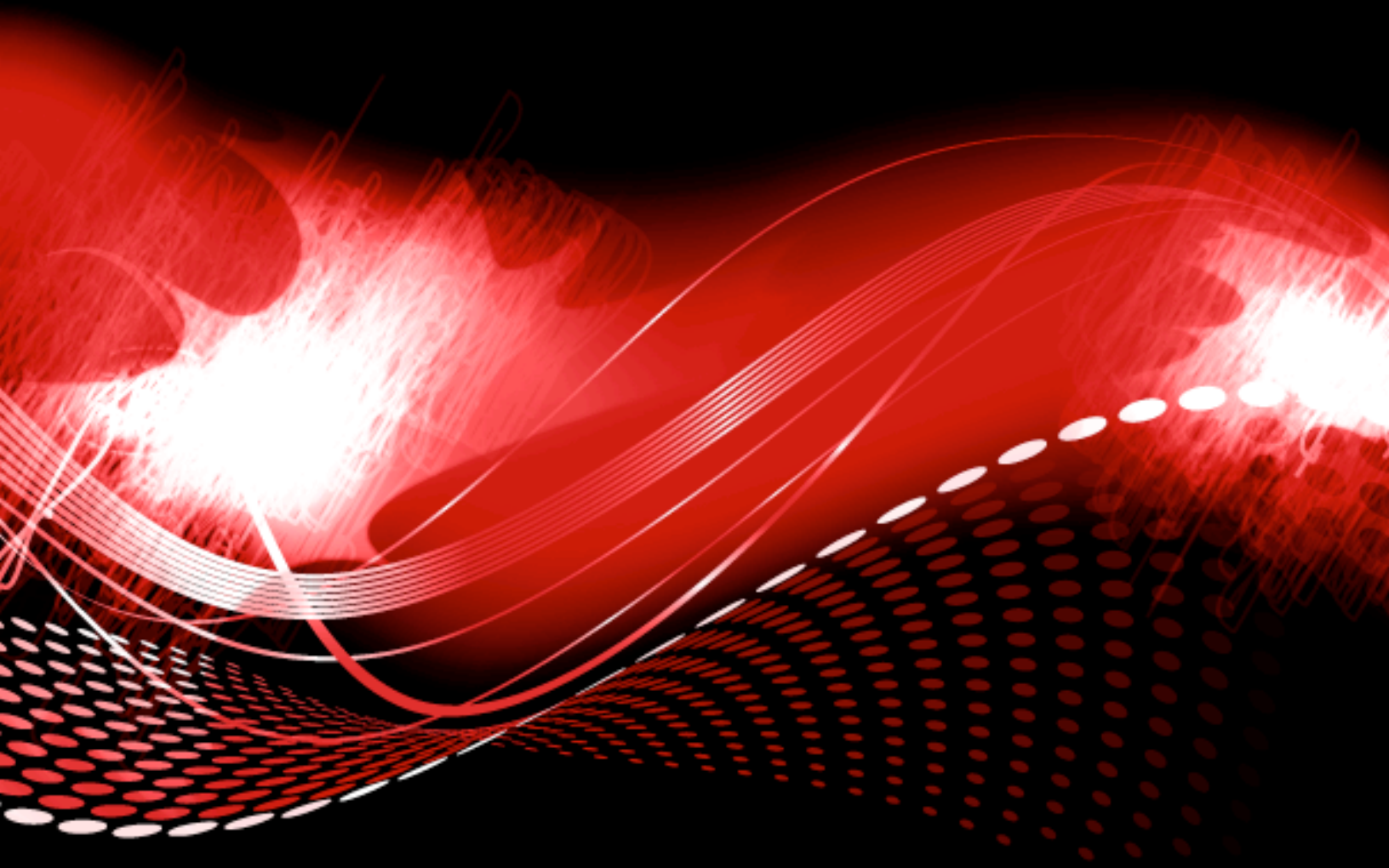
Technology Policies & Procedures

Robert J. (Rob) Rennie, PhD

01.01.2013 – 12.31.2013



Information Technology

Florida State College at Jacksonville

01-01.13 • General Purpose and Organization [Reiman] 8
01-02.13 • Format & Style [Wickline] 9
01-03.13 • Authority for Technology Policies & Procedures [Rennie] 10
01-04.13 • Green IT Policy [Smith] 11
02-01.13 • General Purpose and Organization [Reiman] 13
02-02.13 • Collegewide Technology Committee [Rennie] 15
03-01.13 • CIO Role [Rennie] 17
03-02.13 • Technology Vision [Rennie] 20
03-03.13 • Technology Mission [Rennie] 21
03-04.13 • Technology Charge [Rennie] 22
03-05.13 • Technology Goals [Rennie] 23
03-06.13 • Technology Architecture [Rennie] 24
Figure 3.1: Technology Enablement Model 25
Figure 3.2: Information Levels and Functions Model 26
Figure 3.3: Technology Solutions Provisioning Map 27
03-07.13 • Technology Strategic Planning [Reiman] 28
Figure 3.4: Collegewide and Technology Department Strategic Planning & Budget Development Relationship Model 29
03-08.13 • IT Resource Allocation [Thomas] 30
04-01.13 • Associate CIO Role [Rennie] 32
04-02.13 • CTO Role [Rennie] 33
04-03.13 • Annual ERPM Reporting [Smith] 34
04-04.13 • Budget and Fiscal Analysis [Thomas] 35
04-05.13 • Technology Audits [Smith] 37
04-06.13 • SACS IT Requirements [Lott] 38
04-07.13 • Workstation Standards [Smith] 40

04-08.13 • Server Standards [Smith] 41
04-09.13 • Software Standards [Smith] 42
04-10.13 • SMART Classrooms [Smith] 43
04-11.13 • Classroom Standards [Smith] 45
04-12.13 • Lab Standards [Smith] 46
04-13.13 • Standard and Nonstandard Software Acquisitions [Smith] 47
Figure 4.1: Purchasing Standard and Non-standard Software Collegewide Process 48
04-14.13 • Hardware Acquisition [Smith] 49
Figure 4.2: Purchasing Process 51
04-15.13 • Process Measurement & Functional Evaluation [Reiman] 53
04-16.13 • Computer Crimes & Software Piracy [Smith] 55
Table 4.1: Violations and Liability 61
Table 4.2 63
04-17.13 • TECHNOLOGY APPROVAL DUE DILIGENCE [Rennie] 64
05-01.13 • Project Management Definitions [Reiman] 67
05-02.13 • Project Management Standards [Reiman] 68
Table 5.1: Project File Naming Standards 71
05-03.13 • Applicability & Requirements of Project Management [Reiman] 74
05-04.13 • Financial Reporting by Project [Thomas] 75
06-01.13 • Definition [Reiman] 76
06-02.13 • Structure [Reiman] 78
06-03.13 • Methodology [Reiman] 79
06-04.13 • Development [Reiman] 80
06-05.13 • Testing [Reiman] 81
06-06.13 • Production [Reiman] 82
06-07.13 • Programming Standards [Reiman] 84
06-08.13 • Library Management and Change Control [Reiman] 87

06-09.13 • Documentation [Reiman] 89
07-01.13 • Definition [Martin] 90
07-02.13 • Change Control [Martin] 91
07-03.13 • Production Scheduling [Martin] 92
07-04.13 • Library Management [Martin] 93
07-05.13 • Change Management Standards [Martin] 94
07-06.13 • Operating Environment [MARTIN] 95
07-07.13 • Batch Execution/UNIX Scripts [Martin] 96
07-08.13 • System Programming Services & Support Process [Martin] 97
07-09.13 • Development [Martin] 98
07-10.13 • Acceptance Environments in ORION [Martin] 99
07-11.13 • Production Environment in ORION [Martin] 100
07-12.13 • ORION/Artemis Governance Structure [Martin] 101
07-13.13 • Documentation for Data Operations Center [Smith] 103
07-14.13 • Service Level Agreements [Smith] 104
Table 7.1: Service Level Issues, Contacts and Resolutions 104
07-15.13 • Systems Programming [Martin] 106
07-16.13 • Peer Review [Martin] 107
07-17.13 • Separation of Duties [Martin] 109
07-18.13 • ERP/ORION II [Martin] 111
07-19.13 • Solution Environment [Martin] 112
Table 7.2: Data Systems Solution Environment Products 112
07-20.13 • External Data Extract Requests [Martin] 113
08-01.13 • Physical Environment [Smith] 114
08-02.13 • Network Server System (Server Administration) [Smith] 115
08-03.13 • Operational Range [Smith] 117
08-04.13 • Facilities Support [Smith] 118

08-05.13 • Florida State College Peer-to-Peer File Sharing [Smith] 119
09-01.13 • Physical Access to the NOC [Smith] 120
09-02.13 • ERP Systems Security [Martin] 122
09-03.13 • ERP Applications Security [Martin] 123
09-04.13 • Data Security [Martin] 124
09-05.13 • Root/Sys Admin Access [Smith] 126
09-06.13 • ERP Disaster Recovery [Smith] 127
09-07.13 • Back-up Restore Procedures [Martin] 128
09-08.13 • Evacuation Plan [Adeeb] 129
Table 9.1: Emergency Marshals 133
Table 9.2: Security Officers 133
Table 9.3: Safety and Security Telephone Numbers 134
Table 9.4: Safety/Security Department 134
Table 9.5: Safety/Security Department 134
Table 9.6: Safety/Security Department 135
Table 9.7: Hazardous Materials Notification List 135
09-09.13 • Environment Alarms [Smith] 136
09-10.13 • NIPC/INFRAGARD [Smith] 137
09-11.13 • Firewall Administration [Smith] 138
09-12.13 • Wiring Standard [Smith] 139
10-01.13 • PMBOK [Reiman] 140
10-02.13 • Methodology .Net/Java Architecture [Reiman] 141
10-03.13 • ADABAS References, etc. [Martin] 142
10-04.13 • Natural Programming Guides [Martin] 143
10-05.13 • eXtreme Programming [Reiman] 144
10-06.13 • SCRUM [Martin] 146
11-01.13 • Interruption of Phone Services (System Failure) [Smith] 148

12-01.13 • Definition [Martin] 149
12-02.13 • Structure [Martin] 150
12-03.13 • Development [Martin] 151
12-04.13 • Testing [Martin] 152
12-05.13 • Production [Martin] 154
12-06.13 • DBMS Standards (admin) [Martin] 155
12-07.13 • Confidential college information on Consultant/vendor equipment [MARTIN] 158
13-01.13 • Technology Support Services [Martin] 159
13-02.13 • Voicemail [Smith] 161
13-03.13 • Moves, Adds, and Changes (MAC) [Smith] 162
13-04.13 • Service Request Process [Martin] 163
13-05.13 • ERP System Availability Schedule [Martin] 164
Table 13.1: Batch Processing 164
13-06.13 • Network Login [Smith] 166
13-07.13 • Digital Signatures [Smith] 170
13-08.13 • User Agreement [Smith] 172
13-09.13 • Privacy Agreement (WEB) [Reiman] 174
13-10.13 • HIPPA [Smith] 175
13-11.13 • FERPA [Smith] 179
13-12.13 • Incident Reporting Process [Smith] 182
13-13.13 • Wireless Access [Smith] 185
13-14.13 • Email Policy [Smith] 190
13-15.13 • Florida State College at Jacksonville Content Filtering [Smith] 202
13-16.13 • Website Development: Americans with Disabilities Act (ADA) [Wickline] 203
13-17.13 • Internet Domain Registration and Certificates [Smith] 206
13-18.13 • Drive and Media sanitation and destruction [Smith] 207
13-19.13 • College Fact Book [Lott] 209

13-20.13 • State and Federal Reporting [Lott] 210

Table 13.2: Responsible Parties for Reporting 213

13-21.13 • Rehabilitation Act – Section 508 Compliance [Reiman] 214

01-01.13 • GENERAL PURPOSE AND ORGANIZATION [REIMAN]

Recommended By: Dennis Reiman, AVP, Tech, Associate CIO & CTO

Purpose:

The purpose of the Technology Procedures Manual is to provide a fixed resource reference for standing decisions, practices, rules, processes, guidelines, and general information necessary to the effective and efficient management and operation of technology-related functions.

Description/Procedure:

The Vice President, Technology (CIO) will develop, or cause to be developed, procedures consisting of a title, purpose, procedure description/detail, effective dates, assignments of responsibility, and approvals for practices, standing decisions, methodologies, rules, and similar matters relating to technology at the College.

01-02.13 • FORMAT & STYLE [WICKLINE]

Recommended By: Chrystal Wickline, Multimedia Systems Analyst

Purpose:

The purpose of this procedure is to present the structure (template) of the technology procedures and provide a description of the organization (indexing and categorization) scheme applied to the topics.

Description/Procedure:

The template presented in this procedure will be the only recognized and approved format for technology procedures.

The first number represents the main category, for example, 01 is General. The second number after the hyphen is the order in the main category for which it falls, for example, 02 is the second topic within the General category. Finally, the third number after the period represents the year the policy and procedure is effective, for example, 13 is the calendar year 2013.

Number • Title [Owner's Last Name]

Recommended By: Name, Position Title

01-03.13 • AUTHORITY FOR TECHNOLOGY POLICIES & PROCEDURES [RENNIE]

Recommended By: Robert J. (Rob) Rennie, Ph.D., VP, Technology & CIO

Purpose:

The purpose of this procedure is to provide the specific and general authorities under which the technology procedures have been developed and under which they are enforced.

Description/Procedure:

Florida Statute 240.319 provides for the establishment of policies and procedures governing the use of technology resources in state colleges. The College has general Board Rules and APMs regarding technology. The Technology Policies and Procedures Manual serves as the specific operational implementing structure for Board Rules section 6Hx7-7.X and APM Chapter 07.

01-04.13 • GREEN IT POLICY [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this Policy and Procedure is to define the areas of considerations in the design, and product selection of Collegewide technologies in relation to energy efficiency and environmental responsibility.

Wherever possible, redundant technology services should be consolidated. Servers that can be centralized should have their processes centralized at the Network Operations Center. Applications that need their own environment to work in but do not require the full processing potential of their own server should be moved to a virtual environment such as a VMWare or Zone architecture.

The Network Operations Center should follow green power and cooling architecture templates as provided by www.thegreengrid.org.

Technology equipment purchases, in the Network Operations Center as well as down to the desktop, should be made with energy efficiency in mind. Refresh cycles should bring in more energy efficient systems and push less efficient systems out of the organization. IT hardware vendors should be members of the US Government's Energy Star Program, www.energystar.gov.

Information Technology and Desktop Support leaders should follow the best practices of energy efficiency as outlined by the Climate Savers Smart Computing Initiative, www.climatesaverscomputing.org. Software tools such as Deep Freeze will be provided to the campuses to allow software updates and patches to be provided during operating hours and automate classroom computer shutdowns after hours.

Software purchases should made with waste reduction in mind. If manuals and media are not needed for each install, they should not be ordered. I.T. Maintains a server for master copies of software installation media to reduce the amount of media that needs to be purchased. Most software purchases only need a license to be purchased.

Bulk hardware purchases should keep in mind the packaging options that the individual vendors offer in order to reduce the amount of non-recyclable material.

02-01.13 • GENERAL PURPOSE AND ORGANIZATION [REIMAN]

Recommended By: Dennis Reiman, AVP, Tech, Associate CIO & CTO

Purpose:

The purpose of this procedure is to provide the framework for the Technology Division's organization structure and reporting relationships and present a description of the organization principles applied.

Description/Procedure:

The Technology Division comprises the centralized, or core, information systems and technology-related functions of the College. The Vice President, Technology who also serves as the College's Chief Information Officer (CIO), heads the Technology Division. The Vice President, Technology serves on President's Cabinet and reports to the College President.

Within the Division, functional areas are assigned to Associate Vice Presidents, Directors, Managers, and Leads on the basis of expertise, workload, workflow, and systems-based relationships.

The CIO designates direct reports, a Chief Technology Officer, and a Chief Information Security Officer based on current needs and circumstances, which are affected by several factors including, but not limited to, workload, Collegewide priorities, division priorities, project status, performance, and the overall state of the Division relative to strategic and tactical plans.

The Technology Division is organized through the following principles:

- Flat Structure
- Efficiency
- Skills Matching
- Educational Focus
- Customer Service

The Technology Team organization chart is published in the Strategic Technology Plan and on the team's website. This chart identifies the reporting relationships and position titles within the organization. The current version of the chart can be accessed at http://www.techteam.fscj.edu.

02-02.13 • COLLEGEWIDE TECHNOLOGY COMMITTEE [RENNIE]

Recommended By: Robert J. (Rob) Rennie, Ph.D., VP, Technology & CIO

Purpose:

The purpose of this procedure is to describe the role of the Collegewide technology committee as it relates to the CIO, Associate CIO, CTO, and the technology division generally.

Description/Procedure:

The Collegewide Technology Committee is formed and operates under college APMs and is an important element of the governance process for technology.

The role of the Collegewide technology committee as it relates to the CIO and Associate CIO positions is to provide input regarding specific and global technology issues. The committee is charged with the surfacing of issues relating to all areas of technology as well as reacting to issues presented by technology management. Strategic planning for technology is conducted by technology management but draws upon dialogue and idea sharing with the committee. Additionally, the committee serves as the official Collegewide body for the communication of technology-related concerns, issues, problems, and needs for the College as a whole.

One critical role of the committee is its responsibility to facilitate integration of the campus based committees into the Collegewide structure to ensure communication between the campuses and the Collegewide committee. This is particularly important in planning and needs assessment processes.

The committee role in regards to the CTO is to provide input relative to specific technology needs including all areas of the computing and telecommunications environment and to provide input into the establishment, revision, and enforcement of Collegewide technology standards and the processes related to them.

The committee is also the primary vehicle for the establishment of assessment and evaluation criteria relative to the quality and levels of service provided by the technology division and the degree to which the technology environment meets the needs of the institution and its constituents. As with all other aspects of the technology function at the College, the emphasis of the committee's efforts is in educational technology.

The committee also serves as a collective critic of the daily functioning and operations of the technology division, its effectiveness, and the quality of customer service being provided.

03-01.13 • CIO ROLE [RENNIE]

Recommended By: Robert J. (Rob) Rennie, Ph.D., VP, Technology & CIO

Purpose:

The purpose of this procedure is to detail the responsibilities of the CIO (chief information officer) role at the College.

Description/Procedure:

The Vice President, Technology serves as the College's chief information officer. As such the incumbent is responsible for leadership of all technology at the College.

Primary areas of responsibility are the creation and realization of a technology vision, the development of strategies for achieving the technology vision and completing Collegewide initiatives, and the research and application of new and emerging technologies.

Key activities include design of the technology architecture advocacy for technology needs, approving standards, and the allocation of resources. Additionally, the VP/CIO is responsible for establishing a future focus, developing external relationships and partnerships, advising college leaders and the Board on technology and other issues.

As a cabinet level leader, the VP is further charged with the management of initiatives, expected to serve as an agent of change and Collegewide innovation, and to provide general leadership as appropriate. The VP/CIO has very limited involvement in operational supervision.

The position description for the Vice President, Technology and CIO follows:

As the College's Chief Information Officer, the Vice President, Technology provides Collegewide leadership for all technology and information systems functions and related areas. Areas of responsibility include, but are not necessarily limited to: information systems, instructional technologies and systems, administrative technologies, multimedia development, courseware development and distribution, computer operations, communications networks, computer systems development, telephone systems, digital media production, and video/ television infrastructure.

An employee in this classification must possess extensive knowledge and experience in technology leadership and state-of-the-art technologies, develop and implement a technology vision, and conduct short and long term planning for systems development and technology-related initiatives and must function effectively at the senior executive (cabinet) level.

Characteristic Duties and Responsibilities

- Develops and implements the College's technology vision and architecture.
- Develops policies and procedures for ensuring cost effective provision of academic and administrative technologies and information systems.
- Provides leadership for technology initiatives Collegewide and ensures efficient integration of various systems.
- Manages short and long term planning related to technology; emphasizes college mission in all planning initiatives.
- Identifies emerging technologies for the purpose of incorporating such into college systems, assesses potential value for college use and plans implementations.
- Leads the development and production of modern courseware and multimedia products.
- Identifies, establishes, and monitors computer technology standards; analyzes capacity requirements and provides recommendations for solutions.
- Executive level responsibility for technical infrastructure, support, college application maintenance, computer and network operations, and related areas.
- Coordinates and directs innovative technology research and development, instructional software evaluation, strategic information technology planning, and telecommunications management.
- This position reports to the College President (CEO) and directs senior level staff as assigned.
- Performs related duties as assigned.

Minimum Qualifications

Requires a master's degree in management, leadership, management information systems, educational administration, information technology, educational technology, computer science, or related field. Educational qualifications are to be supplemented by ten (10) years of progressively responsible experience in planning, development, and maintenance of complex multi-location, multi-user information systems or other advanced technologies. The majority of this experience should come from a moderate to large-scale organization, including experience in managing the delivery of technology-based instructional programs.

Experience must include a minimum of five years in senior (executive level) technology management. Preferred qualifications include an earned doctorate and ten (10) years senior technology management experience.

The CIO Role is designed to serve as a strategic leadership position for technology. Operational supervision and management is, to a very large degree, delegated to the Associate CIO, CTO and other senior technology managers.

03-02.13 • TECHNOLOGY VISION [RENNIE]

Recommended By: Robert J. (Rob) Rennie, Ph.D., VP, Technology & CIO

Purpose:

The purpose of this procedure is to present the technology vision of the College as expressed in the technology vision statement.

Description/Procedure:

The comprehensive vision for technology at Florida State College at Jacksonville is based on primary philosophical tenets that emphasize enablement, innovation, creativity, agility, optimization, stewardship, professionalism and above all, excellence. These principles are communicated through the technology vision, in combination with the mission and charge statements and subsequent general goals.

Florida State College will be viewed as a technological leader providing superior access to the resources of scholarship and career preparation through the application of advanced technologies.

The vision statement, as well as the mission, CIO charge, and technology goals is designed to provide focus. It is also intended to lead to the establishment of a positive technology culture that embodies the principles of professionalism and educational focus, emphasizes intelligence and creativity, and leverages teamwork.

03-03.13 • TECHNOLOGY MISSION [RENNIE]

Recommended By: Robert J. (Rob) Rennie, Ph.D., VP, Technology & CIO

Purpose:

The purpose of this procedure is to present the technology mission of the College as expressed in the technology mission statement.

Description/Procedure:

The Mission of the Technology Department is to provide the highest quality technological resources possible to the College to support achievement of the College's mission, vision, goals, and objectives.

The major function of the mission statement is to support the integration of the technology division into the College's mission.

03-04.13 • TECHNOLOGY CHARGE [RENNIE]

Recommended By: Robert J. (Rob) Rennie, Ph.D., VP, Technology & CIO

Purpose:

The purpose of this procedure is to present the charge of the technology division of the College as expressed in the CIO's charge statement.

Description/Procedure:

The Technology Team at Florida State College will pursue every technological advancement of promise for the improvement of the educational process, engage in continuous improvement of quality of services provided to clients, and conduct business in a collaborative and instructionally-focused manner.

The CIO's charge to the technology team (division) is delivered for the purpose of establishing tone and priorities of focus as a basis of operation and foundation for development and advancement of the division.

03-05.13 • TECHNOLOGY GOALS [RENNIE]

Recommended By: Robert J. (Rob) Rennie, Ph.D., VP, Technology & CIO

Purpose:

The purpose of this procedure is to present the three technology goals of the technology division of the College.

Description/Procedure:

Florida State College's comprehensive technology vision will be realized through the achievement of three general goals:

Technology GOAL 1: Achieve and Maintain an Educational Focus

This goal is achieved by deliberately directing all resources toward students, their transactions and interactions with the college, and the processes that most directly affect them.

This focus includes emphasizing the lab and classroom computing environments but also includes faculty computing, instructional software, courseware, and individualized portal development. Additionally, this goal requires effective resource stewardship that ensures cost effective and efficient solutions, including cloud and other emerging technologies, that optimize the resources available to the college.

Technology GOAL 2: Technological Leadership and Value Creation

Achieving a technology leadership position, and maintaining it, is achieved through the application of technology as a value creation engine. This includes the enrichment of business processes in the higher education value chain, the enablement of new business through advanced technology capabilities, and direct support of organizational advancement through early adoption of significant value-creating technologies.

Technology GOAL 3: Technological and Organizational Agility

Agility is best achieved through the establishment of an overall architecture that provides a manageable level of platform/solution independence, rich platform selection, and a workforce based on intellectual horsepower rather than specific skills.

03-06.13 • TECHNOLOGY ARCHITECTURE [RENNIE]

Recommended By: Robert J. (Rob) Rennie, Ph.D., VP, Technology & CIO

Purpose:

The purpose of this procedure is to provide a general model of the College's technology architecture.

Description/Procedure:

The College's technology architecture is built on a foundation formed by three models. First is the technology enablement model. Based on the belief that value is created through technology use, the enablement model provides for ubiquitous access and the creative development of applications that accrues from it. It is summarized in the following bullets and represented by the accompanying figure.

Enablement Model:

- Provide the Technology, applications evolve from access and use
- Faculty first, then students
- Reasonable sustainable standards
- Self sufficiency model
- Solid support and training
- Exceptional digital resources

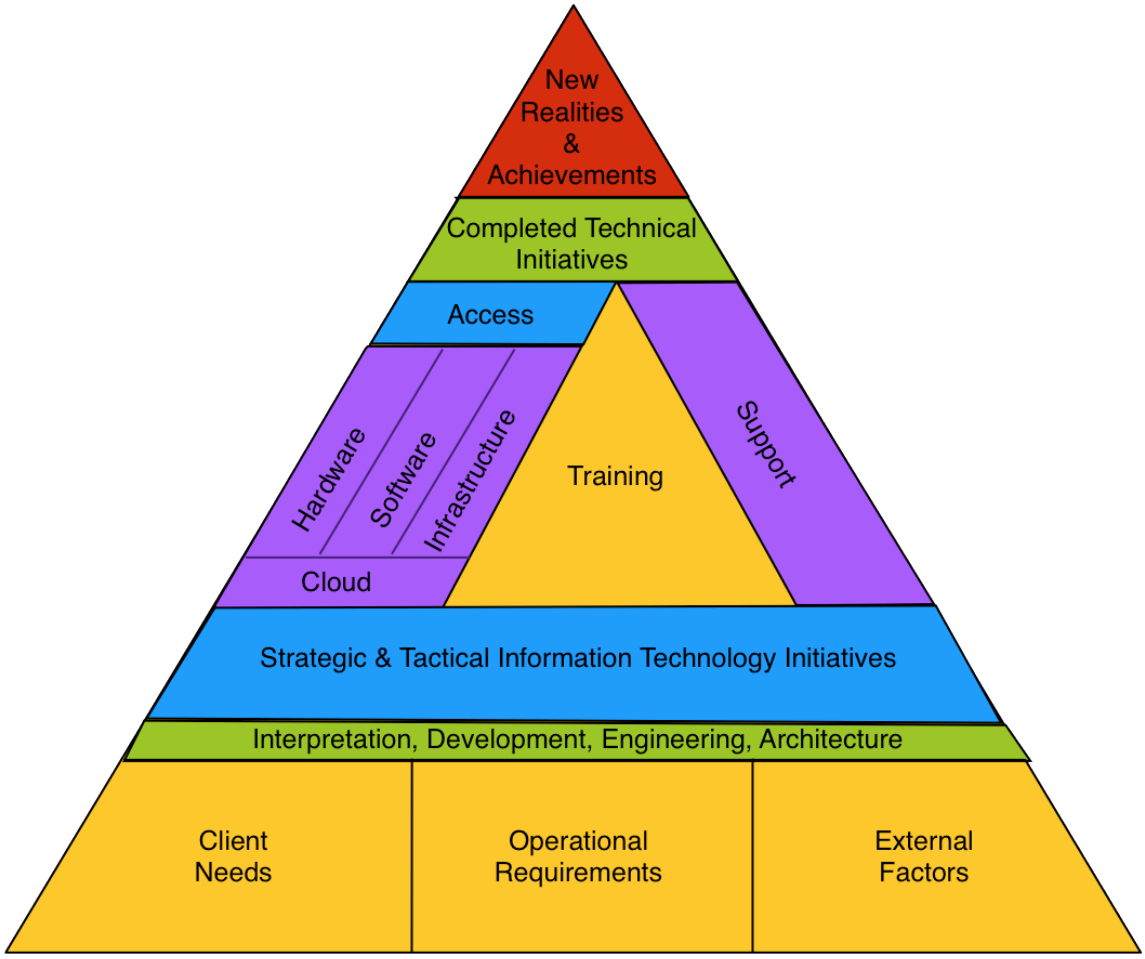


Figure 3.1: Technology Enablement Model

The second foundational element of the technology architecture is the information levels and applications model depicted in the following figure. Note that the back-end, or transaction engine, serves as the base upon which all information levels and attendant functions and applications are built.

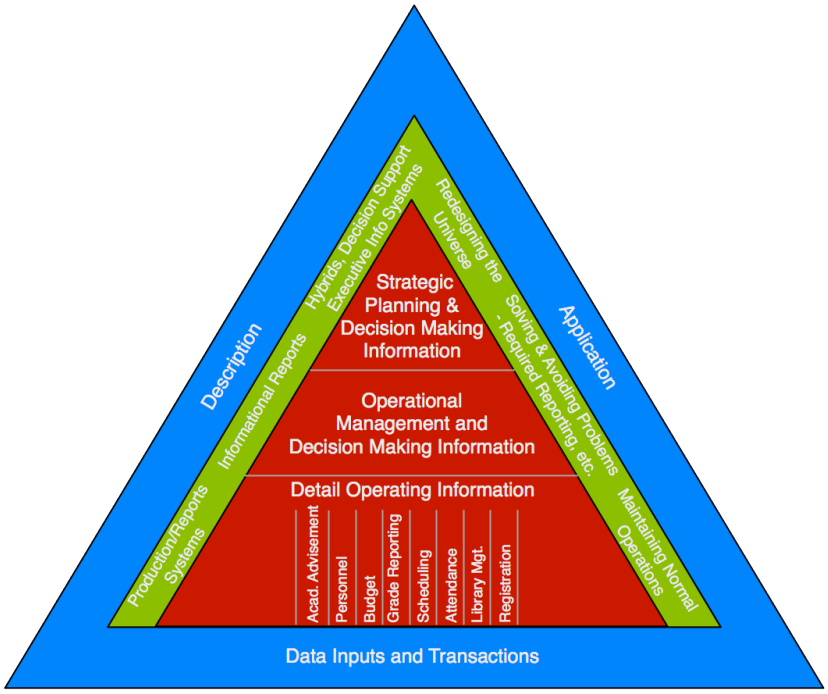


Figure 3.2: Information Levels and Functions Model

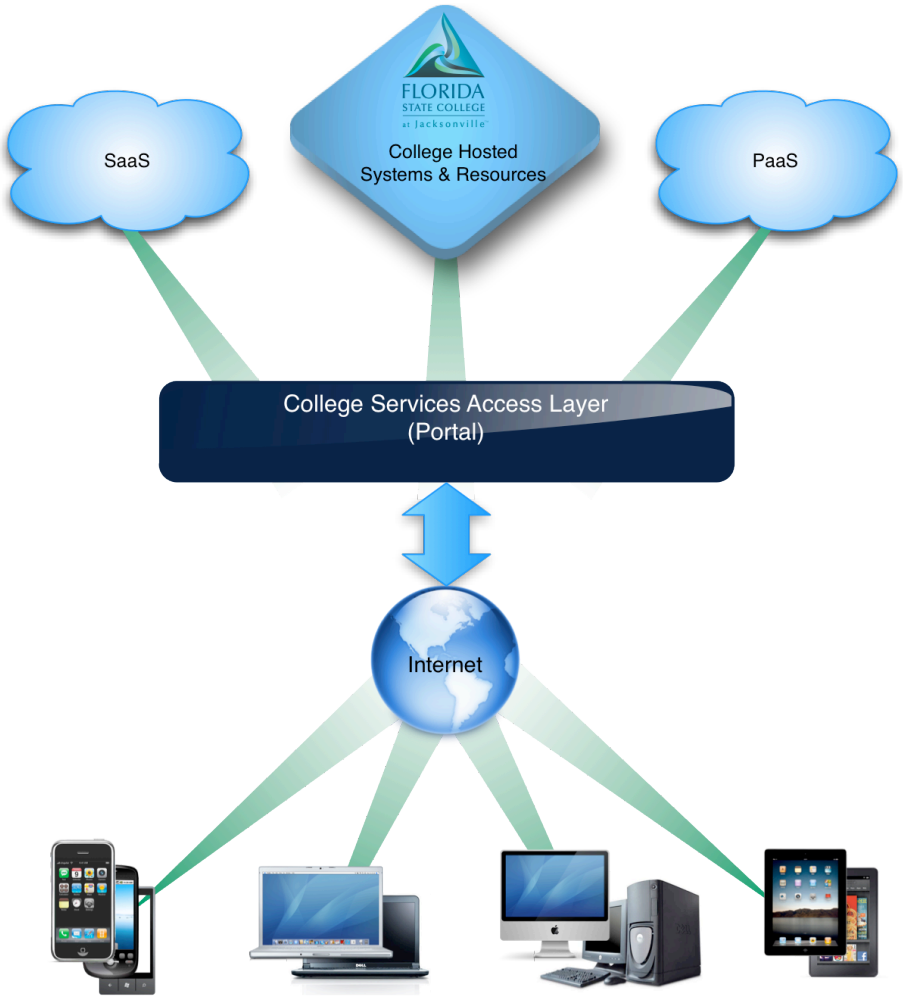


Figure 3.3: Technology Solutions Provisioning Map

The third and final foundational element of the architecture is the technology solutions provisioning model depicted in the graphic above. Note the basis of this architecture is the provision of shared resources and systems without regard to their physical location. It blends cloud-based software and platform as a service solutions and resources with college-hosted resources in one aggregate architecture.

03-07.13 • TECHNOLOGY STRATEGIC PLANNING [REIMAN]

Recommended By: Dennis Reiman, AVP, Tech, Associate CIO & CTO

Purpose:

The purpose of this procedure is to describe the strategic planning process of the Technology Division and the resultant publication of the College's strategic technology plan.

Description/Procedure:

Planning for technology at the College is a collaborative effort divided into two major categories, strategic and tactical. Tactical planning is more operational in nature and is the responsibility of functional managers and supervisors. This topic is covered under project management procedures and relates to the management of approved work and the implementation of strategic plans once approved/adopted. The time frame covered is generally one year or less. The strategic planning process deals with long-term (up to five years) issues and general matters of architecture and direction as opposed to detailed projects.

The strategic planning process for the College is based on the development of strategic initiatives. To a large degree, technology strategic planning follows this practice. However, additional collaborative work is done through the Collegewide technology committee, task forces, and technology managers to establish long-term direction, priorities for resource allocation, and the incorporation of emerging technologies into the architecture. The products of the strategic planning process are the regular budget requests included in the College budget process, strategic initiative proposals, and the College's published Strategic Technology Plan. The Strategic Technology Plan is updated as needed to reflect the current technology vision, mission and goals; the architecture, management and structure, fiscal resources, and five-year outlook; and other significant information related to the College's technology position and plans for the future. The current version of the Strategic Technology Plan can be accessed at the Technology Team web site, http://www.techteam.fscj.edu.

Figure 3.4 depicts the relationship between the collegewide and technology department planning and budgeting processes.

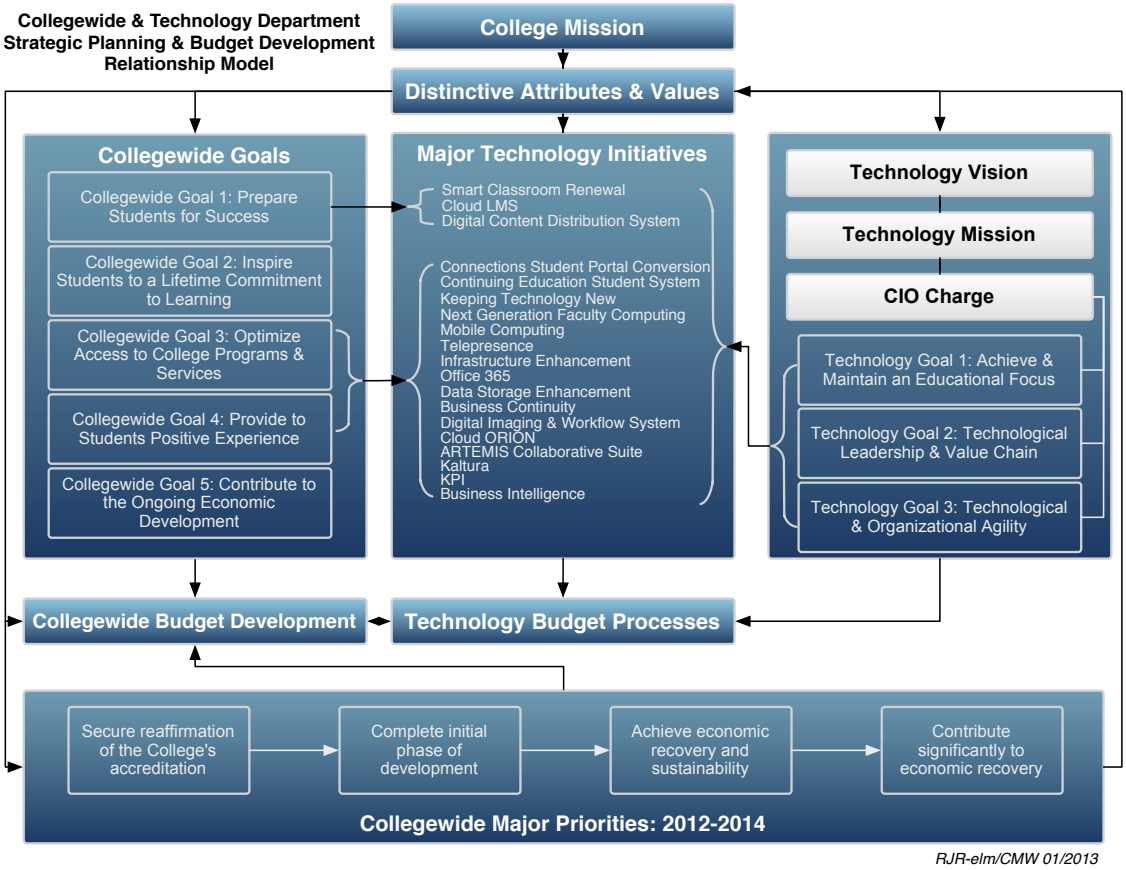


Figure 3.4: Collegewide and Technology Department Strategic Planning & Budget Development Relationship Model

The responsibilities associated with the strategic planning process for technology are as follows:

- Production, publication, and distribution of the Strategic Technology Plan are the responsibility of the CIO.
- Operational technology needs and performance, customer service, and new/revised service level planning is the responsibility of the Associate CIO with specific area assignments for functional area managers and supervisors. This includes a five-year outlook and fiscal analysis.
- Planning for technology standards, the development of roadmaps, and long term refresh and implementation schedules is the responsibility of the CTO.
- The process is intended to ensure involvement of all college constituents in a collaborative fashion emphasizing support of the educational mission.

03-08.13 • IT RESOURCE ALLOCATION [THOMAS]

Recommended By: Kelly Thomas, Director, Technology Administration

Purpose:

The purpose of this Technology Procedure is to describe the resource allocation process for information technology within the College.

Description/Procedure:

On a yearly basis with input from the College's community representatives, the Information Technology Department shall formulate information technology allocation plans. Approvals are secured as part of the College's overall annual budget adoption process.

- Information Technology Resources Allocation
  - Allocation of technology resources for academic purposes, for use by faculty, academic staff, and students under the direction of faculty, shall be a primary priority within the Technology Department.
  - Allocation of Information Technology resources to academic and administrative functions shall support the college's goals, initiatives and objectives for a given year, as well as the College's strategic and tactical technology plan.
  - The College's Technology Department formulates plans for technology investments on an annual basis, based on College needs and input from faculty, students, staff and administrative areas. Data may be collected directly, through representatives, or through the budget development process.
  - Total information technology resources available in a given year will vary depending upon State Appropriations, funding for special technology-related programs, and technology-related grant funding as well as Collegewide priorities.

- Review & Measurement of Information Technology Allocations
  - The college shall review information technology allocations on an annual basis and report actual results and plans to the President's Cabinet and Board of Trustees as part of the annual operating budget approval process.
  - In a given year, allocations of available information technology resources to academic and administrative purposes may each vary depending upon specific goals and circumstances of the College, such as State and Federal mandates, or failures or breaches in mission critical technology systems.
  - The college shall manage its information technology allocations such that the target allocation to academic technology systems and initiatives will approximate fifty-five (55) percent in a given five-year period, beginning in the fiscal year 2002-2003 Budget.
- Reconciliation & Remedial Action
  - The President and Cabinet shall recommend to the Board of Trustees special technology spending and allocation action in the event allocations to academic do not approximate fifty-five (55) percent in a given five-year period. Any action may be deferred during times of fiscal exigency.

04-01.13 • ASSOCIATE CIO ROLE [RENNIE]

Recommended By: Robert J. (Rob) Rennie, Ph.D., VP, Technology & CIO

Purpose:

The purpose of this procedure is to describe the Associate CIO role at the College and detail its responsibilities.

Description/Procedure:

The Associate CIO at the College is a role designated by the CIO to a senior technology administrator, typically executive (AVP) level. The purpose of the role is to provide daily operational management for the technology division of the College, lead special projects, and represent the CIO, internally and externally, as appropriate. This role is above and beyond the typical duties of the administrator to whom it is assigned.

Qualifications

The Associate CIO assignment is based on exceptional leadership ability and requires a global understanding of all technology related functions.

04-02.13 • CTO ROLE [RENNIE]

Recommended By: Robert J. (Rob) Rennie, Ph.D., VP, Technology & CIO

Purpose:

The purpose of this procedure is to describe the CTO (chief technology officer) role at the College.

Description/Procedure:

The chief technology officer (CTO) role is a leadership role assigned to a senior technology manager by the CIO. The purpose of the role is to attend to the detailed coordination and integration of the major technology components and functions of the College's technology architecture as established by the CIO. Major focus of the role includes recommending the adoption and implementation of new technologies, planning the implementation of new practices, processes, systems, and technologies; establishing and enforcing technology standards; and negotiating with vendors and managing resultant contracts. The CTO is responsible for the creation and management of the College's technology roadmap.

Qualifications:

The CTO assignment is based on an exceptional working knowledge of a broad array of technologies as well as understanding of global technology trends and the ability form a comprehensive technology roadmap.

04-03.13 • ANNUAL ERPM REPORTING [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this Technology Procedure is to identify information as it pertains to Enterprise Resource Planning and Management Report.

Description/Procedure:

The Enterprise Resource Planning and Management and the College's submission requirement report (ERPM) are submitted to the Executive Office of the Governor, House Fiscal Responsibility Council, and Senate Budget Committee through the State Technology Office via the FCCS Office. Within this report, information concerning Information Technology at Florida State College @ Jacksonville is submitted which includes:

- Data Architecture
- Hardware Inventory
- LAN/WAN Information

The form in which this information is collected may be amended. It is the responsibility of the Associate CIO to ensure accurate and timely submission of the Technology Division requirement of this report and to ensure that the data submitted reflects, to the greatest extent practical, the technology at the College.

04-04.13 • BUDGET AND FISCAL ANALYSIS [THOMAS]

Recommended By: Kelly Thomas, Director, Technology Administration

Purpose:

The purpose of this Technology Policy and Procedure is to provide information on budget and fiscal analysis procedures within Technology Department.

Description/Procedure:

The Technology Department operates within the Board of Trustee Rules and resulting Administrative Procedure Manual (APM) for the Purchasing and the Finance Department(s) and in accordance with the Purchasing Department parameters defined by the Purchasing Department Manual.

Information Technology Zero-based Budget Plans with Decision Packages

The Technology Department follows the budget submission calendar and process as defined by the Finance Department within the College. Specific to Major Technology initiatives is the use of a zero-based budget-planning model. The model includes shared budget decision-making, the development and application of integrated strategies, and a prescriptive project-based allocation of resources as a way of achieving established goals and objectives. Together with project financial needs and ROI analysis the information is aggregated into a decision package.

Decision Packages are used by the Technology Department to present a full business case and fiscal analysis of major initiatives. For all single- or multi-year decision packages, the following information is provided for consideration of funding:

- Estimated Expenditures
- Savings
- Revenue
- Cash flow
- Breakeven Point
- Net Present Value (NPV)
- Internal Rate of Return (IRR)

- Return on Investment (ROI)
- Economic Value Added (EVA)

Analytical Tools

Zero-based budgeting requires functional units to identify, develop, and submit decision packages for each major new initiative. Leaders of each initiative are responsible for creation of the decision package. For operational expenditures as well as new major initiatives, the Technology Department has implemented analytical tools to complement the budget and financial analytical capabilities of the Orion2 ERP System. Central to these tools is the use of project codes to link departmental budgets and operational and capital expenditures. Project codes are alpha-numeric, one letter, two digits, assigned sequentially.

Using project codes, each project expenditure is associated with technology budgets and general ledger codes (GLCs). This practice provides for post-fiscal year and post-project analysis of expenditures associated with operating costs and decision packages. The zero-based budgeting and decision-package approach towards budget proposal, funding and implementation provides for monitoring, evaluation of objective achievement, and continuous quality improvement in overall project management.

04-05.13 • TECHNOLOGY AUDITS [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this policy is to provide continuing efforts and responsibility for quality assurance in the areas of systems security, integrity, hardware vulnerability and availability of computer devices owned by or connecting to the Florida State College network.

Description/Procedure:

Audits will be conducted by internal and external sources. The Technology Department on a continual basis should perform limited internal audits, such as security and hardware vulnerability. An unbiased vendor shall conduct external audits. External audits should include, but not be limited to, the Gramm-Leach-Bliley Act, Sarbanes-Oxley Act, and Patriot Act. External auditors will perform a regulatory review through interviews, document review and testing. These findings will be validated to prove the existence or absence of appropriate controls.

Deficiencies discovered during the audit process will be assessed and dealt with appropriately to assure quality, integrity, and security within the systems.

04-06.13 • SACS IT REQUIREMENTS [LOTT]

Recommended By: Theresa Lott, Executive Director, College Data Reporting

Purpose:

The purpose of this Technology Policy and Procedure is to provide information for the accreditation requirements of the Southern Association of Colleges and Schools (SACS) as it pertains to Information Technology resources at the College.

Description/Procedure:

The Southern Association of Colleges and Schools Commission on Colleges (SACS) is the regional body for the accreditation of degree-granting higher education institutions in the Southern states. It is necessary that the Information Technology Department meet the standards of accreditation as defined by SACS [1].

There are two SACS accreditation standards related to Information Technology in post-secondary institutions: "Institutional Effectiveness" (3.3) and "All Educational Programs" (3.4) as follows:

Institutional Effectiveness (3.3.1): The institution identifies expected outcomes, assesses the extent to which it achieves these outcomes, and provides evidence of improvement based on analysis of the results in each of the following areas:

- 3.3.1.1 Educational programs, to include student learning outcomes.
- 3.3.1.2 Administrative support services.
- 3.3.1.3 Educational support services.
- 3.3.1.4 Research within its educational mission, if appropriate.
- 3.3.1.5 Community/public service within its educational mission, if appropriate.

[1] (2011). Commission on Colleges. Southern Association of Colleges and Schools.

Educational Programs (3.4.12): The institution's use of technology enhances student learning and is appropriate for meeting the objectives of its programs. Students have access to and training in the use of technology.

Each year the College's Campuses and Centers submit academic software requests pertinent to instruction through the Lab Replacement Project. Computer hardware replacement is scheduled for a four-year replacement cycle although high-end special labs may have its computer hardware replacement more often with existent hardware cascaded to older labs.

Other avenues for input and participation in technology needs and definition exist within the College infrastructure. The Collegewide Tech Committee provides a forum for members of the College community to bring forth discussion on issues relevant to technology and technology-use. User groups and student government representatives are among the constituencies that define many of the functions of the employee and student portals, Artemis, and Connections.

04-07.13 • WORKSTATION STANDARDS [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of the procedure is to provide information as it pertains to the standardization of college workstations.

Description/Procedure:

The Information Technology Division, Directors of Administration Services (DAS) and campus technology staff support workstation standards as defined by the Information Technology Division. On a college wide basis, "Workstation" typically refers to desktops that are used by faculty and staff as it relates to college functions.

Standard

Information Technology Division managers will meet with the campus Directors of Administrative Services (DAS) and campus technology staff, as prescribed by the CTO, to discuss and identify workstations. Acquisitions of these products are accomplished through traditional college purchasing processes with inherent technology approvals required at the time of submission. At the current time the college is implementing a 5-year replacement cycle.

- Refer to the Minimum New Hardware & Software Requirements & Minimum Supported Existing Hardware & Software Configuration
- All workstations are to be placed in the approved STUDENT or FSCJ Domains
- All workstations must adhere to the approved naming convention. Example dwc-staffid for staff and dwc-room#-# for classrooms.
- All workstations must have the appropriate inventory agent software and Sophos Antivirus install on them.
- All Workstations must allow Domain Administrators access to manage them.
- All workstations must allow for periodic updates and patches.
- The AVP of Technology Operations must approve any exceptions to the above items.

04-08.13 • SERVER STANDARDS [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this section is to identify current standards for network servers on Florida State College production networks.

Description/Procedure:

All servers connected to the Florida State College network infrastructure are required to meet specifications set by the Technology Operations department. It is the responsibility of this department to maintain current standards to ensure optimal performance and reliability. The Technology Operations department prior to ordering shall approve server purchases. Technology Operations must also grant approval before moving servers into the production environment.

The following specifications are accepted as minimal:

- Licensed operating system w/ the latest patches dual power supplies rack mounted
- RAID 5 hardware configurations for data, RAID 1 for OS (RAID 1 may also be used for data if drives are limited)
- Dual NICs
- Appropriate backup software determined by Backup Administrator
- Managed Antivirus
- Three year warranty – minimum next day, four hour preferred

*Servers used in actual lab teaching environments are exempt from this policy. Lab servers must not interfere with normal LAN/WAN operation.

04-09.13 • SOFTWARE STANDARDS [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this Technology Policy is to identify information pertaining to software standards.

Description/Procedure:

To ensure current versions and consistent licensing, the College's standard productivity software, Microsoft Office, is obtained through the annual Microsoft Campus Software Agreement. Staff computers are to maintain consistency in using the most current versions of this software. Annual contracts are negotiated with Microsoft and other publishers to provide the College the right to acquire licenses for software through defined vendors. Whenever possible, site licenses are obtained in order to make efficient use of fiscal resources.

Academic units will define software for academic programs. The campus DAS will approve and submit software requests on behalf of their academic units for the following fiscal year by April 30th to the Director of Technology Administration.

If the license contract also allows faculty and staff to use software titles on their home computers for college related work, installation media will be made available through the most efficient means. If the license allows for a discounted cost for faculty and staff to use software titles on their home computers, instructions will be made available on how to receive this discounted purchase.

Non-standard software may be used only if tested for system compatibility and approved by the CTO.

Current Software Standards:

- Microsoft Windows 8 or Mac OSX Mountain Lion
- Microsoft Office 2012 for Windows or 2011 for Mac
- Microsoft IE 9.0 or Safari 6
- Sophos Antivirus or Microsoft Endpoint Protection

04-10.13 • SMART CLASSROOMS [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this Technology Procedure is to identify information relating to the creation of Smart Classrooms.

Description/Procedure:

The College strives to facilitate technology-enhanced instruction in a number of ways, not the least of which is development and enrichment of the learning environment. The College's Smart Classroom Initiative is designed to provide instructional technology in classrooms for use by the faculty in traditional and hybrid courses. Group training is provided by the office of Professional Development; the Center for the Advancement of Teaching and Learning, with continuing, remedial and one-on-one assistance through the Learning Innovations Area. Technical support and consulting, as needed, is provided through campus technical support and the Enterprise Systems Group.

The Smart Classroom standards are identified periodically to ensure that appropriate technology is available.

Under the direction of the Associate Vice President of Technology Operations, Smart Classroom standards are evaluated in the fall of each year. Newly acquired Smart Classrooms should adhere to the Technology Hardware Standards Guide, construction should adhere to the Technology Construction Standards Guide and will include:

- Short Throw Digital Projector
- Apple iMac with Mac OSX and Windows 7
- Apple TV
- Crestron Scaler
- Creston Control
- Distribution amplifier
- Plenum cable set

Smart Classrooms are used to present a variety of multi-media content for the purpose of enhancing course quality, thoroughness, and the ability to meet the multi-sensory learning needs of students.

04-11.13 • CLASSROOM STANDARDS [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of policy is to provide information as it pertains to the technological standardization of college classrooms.

Description/Procedure:

As a technology standard, classrooms will be designated as “regular” or “smart” classrooms.

Regular classrooms will be equipped with the following:

A minimum of 1-½ cat 6 network connections per computer in the room.

Smart Classrooms will be equipped with the following:

Please reference Policy and Procedure 04-10 – SMART Classrooms

04-12.13 • LAB STANDARDS [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this Technology Policy is to identify information pertaining to standards for computer lab technology equipment.

Description/Procedure:

Computer labs shall be under the direct responsibility of the campus DAS and maintained by the campus Integrated Systems Specialist. Each campus computer lab shall be evaluated on an annual basis to ensure it meets the needs of the programs utilizing the lab. Each campus DAS will need to develop an "equipment life-cycle plan" for each lab. This plan should include provisions to cascade equipment from labs requiring the latest technology to labs with older computers requiring less technology. All lab equipment must meet the College minimum hardware standards.

Requests for lab equipment replacement for the following fiscal year shall be made to the Director of Technology Administration by February 1st. Requests will then be assessed to prepare budget proposals.

Lab software requests for the following fiscal year shall be made to the Director of Technology Administration by April 30th. Requests will then be assessed to prepare budget proposals.

The College will use Thin-Client technology for campus labs where feasible. Using this technology will extend equipment life cycle, reduce support needs, improve software refresh, and reduce overall technology costs.

04-13.13 • STANDARD AND NONSTANDARD SOFTWARE ACQUISITIONS [SMITH]

Recommended By: Kelly Thomas, Director, Technology Administration

Purpose:

The purpose of this Technology Policy and Procedure is to identify information pertaining to software acquisition and to provide documentation of the process to be followed in the acquisition cycle. Reference policy and procedure 04-17 – Technology Approval Due Diligence for description of the due diligence process of the technology division in the selection and approval of technology solutions.

Description/Procedure:

Standard Software Acquisition

The College's standard software acquisitions are those obtained through the Microsoft Campus Software Agreement, Apple Education Licensing Program, or other Collegewide license. Each year a contract is negotiated with Microsoft, Apple, and other publishers, which provides the College the right to acquire licenses for software through defined vendors. The contract agreement also allows faculty and staff to use certain software titles on their home machines for college related work.

Academic units define standards for academic programs. Whenever possible, site licenses are obtained in order to make efficient use of fiscal resources.

Non-standard Software Acquisition

Academic units or business units who provide services to the College community do not typically use non-standard software. However, occasional program-specific (such as health career programs), supplementary (in certain tutoring applications), or pilot program software acquisition is necessary. Approval from the Director, Technology Administration is required prior to any non-standard software acquisition that exceeds the capital software cost threshold, is intended for use by students, or will be installed on a server. The Director, Technology Administration will work with the AVP of Technology Operations to assure compatibility of the software with the current environment.

The process for purchasing standard and non-standard software collegewide is depicted in the following process:

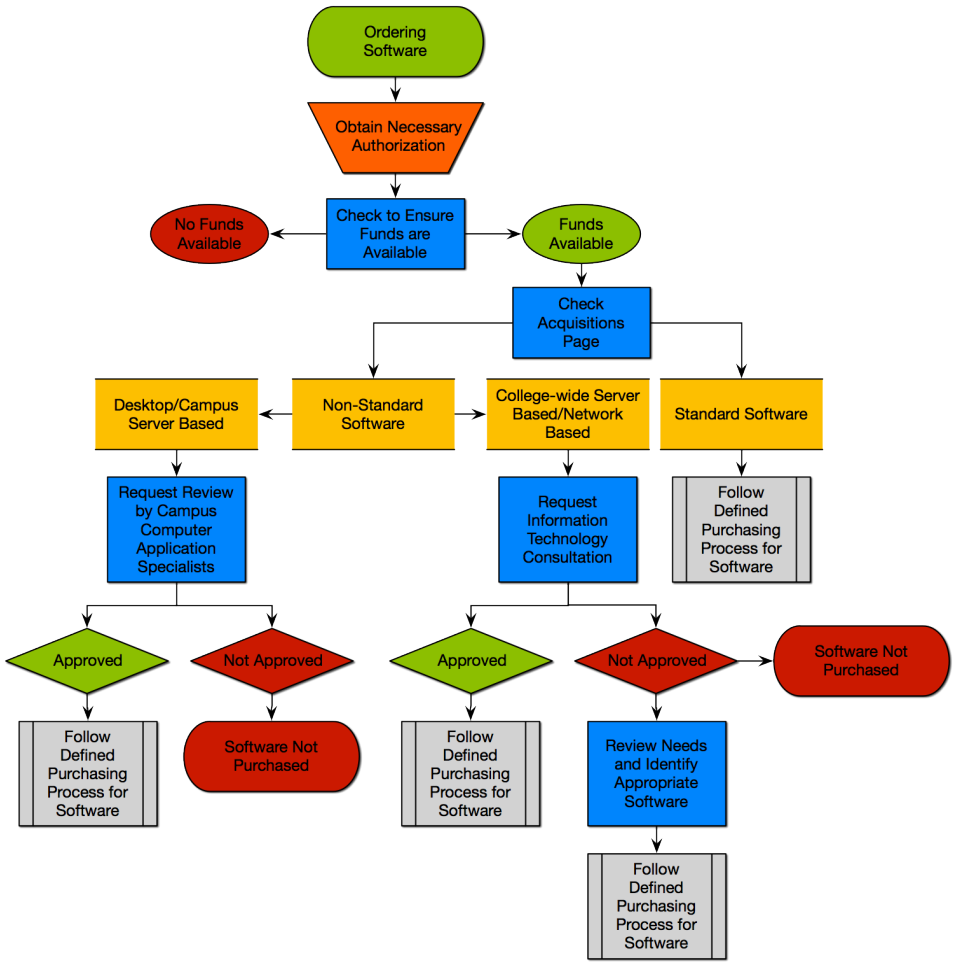


Figure 4.1: Purchasing Standard and Non-standard Software Collegewide Process

In addition, the following information should be contained within the software acquisition request:

- Course name and title, or non-academic function as applicable including version number
- Responsible individual(s)
- Number of licenses requested

04-14.13 • HARDWARE ACQUISITION [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this Technology Policy and Procedure is to provide information as it pertains to standard and non-standard hardware acquisition Collegewide. Reference policy and procedure 04-17 – Technology Approval Due Diligence for description of the due diligence process of the technology division in the selection and approval of technology solutions.

Description/Procedure:

The College will provide appropriate technology to all faculty, staff, and administrators, which may include, at the discretion of management, desktop and mobile devices [including but not limited to laptops, tablets (iPads), converged devices (iPhones), cellular data cards], and other technology resources as deemed appropriate.

The Information Technology Division currently supports three hardware platforms (enterprise, server, and desktop/mobile) within its architecture. On a college wide basis, hardware acquisition typically refers to servers and desktops, routers for networks, and telecommunications-related products.

Standard

Information Technology Division managers meet with the campus Directors of Administrative Services (DAS) and campus technology staff, to discuss and identify desktop and peripheral standards. The Learning Innovations team in concert with Multimedia Technology personnel defines standards for smart classrooms and all audiovisual equipment. Acquisitions of these products are accomplished through traditional college purchasing processes with inherent technology approvals required at the time of submission.

Server configuration requirements and infrastructure products are the responsibility of the AVP of Technology Operations who will provide consulting and specifications for all telecommunication-related projects.

Currently, an expansion to the well-established partnership with Dell and Apple is in place for the provision of desktop equipment and each vendor provides websites with Academic pricing. The Director, Technology Administration may negotiate pricing, beyond these discounts, for bulk purchases.

Cell phone and converged device acquisitions are subject to the device approval process, a subset of the cell (or converged device) cell phone allowance process. An employee whose role has been identified by their cabinet member as requiring a cell phone allowance may be provided one. The appropriate cabinet member brings the signed allowance request to Cabinet for consideration, if approved, the form is forwarded to the finance department for processing and the allowance will be paid as a taxable allowance through the payroll process. There is no guarantee of continued approval of any allowance.

Requests for devices may also be considered through this process. Devices may include cell phones, smart phones, converged data devices, and cellular-capable tablets. The College may purchase the device directly or, preferably, the employee may purchase the device and be reimbursed through the standard business expense reimbursement process. It is recommended that managers encourage employees to leverage their carrier discounts for the device purchase and limit devices to no more than once every two years in frequency. Approved devices purchased by an employee, for which they are reimbursed as a business expense, are owned by the employee. The College has no responsibility to the employee regarding such devices, their performance, reliability, support, or useful life.

Non-standard

Any non-standard technology procurement requires consultation with and approval from the appropriate Information Technology functional area.

Projects requiring specific network connections and server support must be first reviewed and approved by the AVP of Technology Operations as well as Network and other telecommunication needs. Either, the Learning Innovations team and/or Multimedia Technology personnel review audiovisual projects as appropriate.

The process for purchasing standard and non-standard hardware college wide is depicted in the following process:

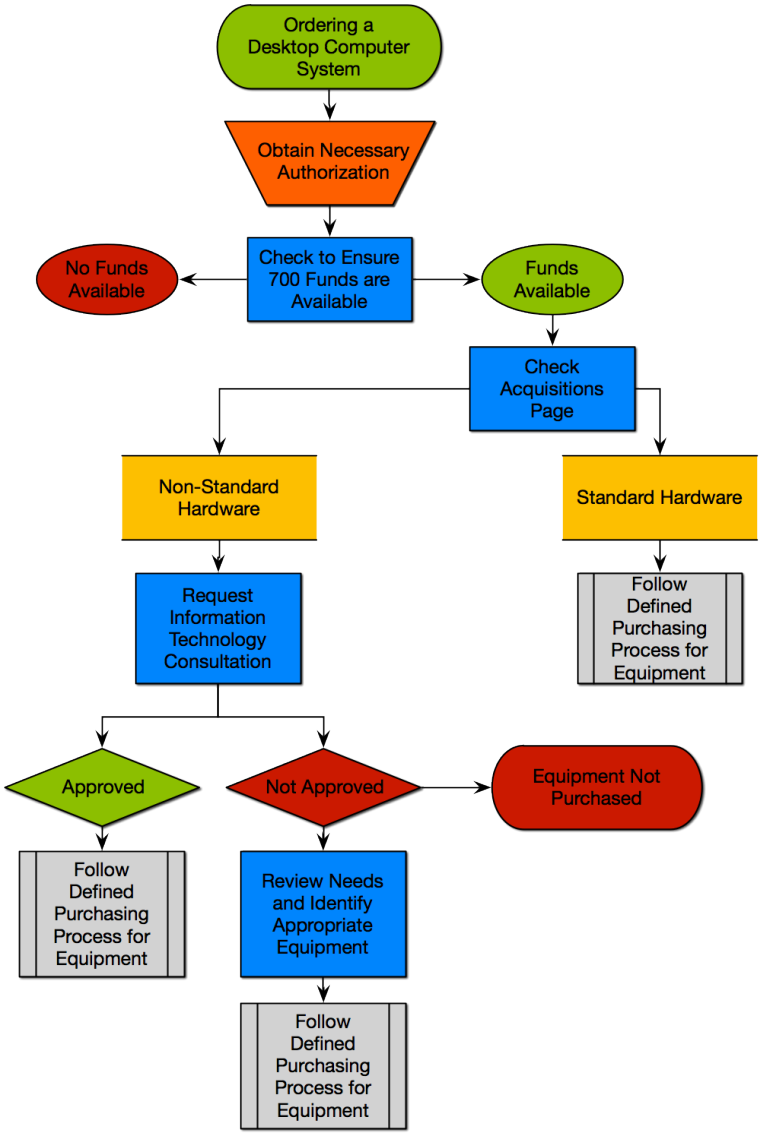


Figure 4.2: Purchasing Process

In addition, the following information should be contained within the hardware acquisition request:

- Request for hardware and amount(s)
- Responsible individual(s)

- Academic or non-academic function as applicable

04-15.13 • PROCESS MEASUREMENT & FUNCTIONAL EVALUATION [REIMAN]

Recommended By: Dennis Reiman, AVP, Tech, Associate CIO & CTO

Purpose:

The purpose of this Technology Policy and Procedure is to provide information on the framework for process measurement and functional evaluation as used in the Technology Division.

Description/Procedure:

The basis for process measurement and functional evaluation within the Technology Division is rooted in the organizational structure, driving philosophy; personnel, management, facilities and operational processes used by the department to delivery its services to the College community. Much if not all of this information is contained within the Technology Policies and Procedures, and serves as the framework from which the process measurement and functional evaluation takes place.

To continue to effectively contribute towards the College's goals, the existing framework for process measurement and functional evaluation includes:

Project management

The objectives of project management are to set and meet achievable commitments regarding cost, schedule, quality, and function delivered—as they apply to operational goals or new projects. The key goals are to create achievable plans and in tracking the status and progress of its projects relative to its plans and contributions.

Process management

The objectives of process management are to ensure that the processes within the division are performing as expected, to ensure that defined processes are being followed, and to make improvements to the processes so as to meet objectives.

Outcomes assessment

The objectives of outcome assessments are to ensure customer acceptance of and satisfaction with the project. The issues of greatest concern relate primarily to the attributes of the project process – planning, budgeting, communication, responsiveness, performance, and so forth. Information about these attributes and customer satisfaction is important to assessing the attainment of project and department goals. Following the completion of projects, functional areas within the Technology Division are responsible for distribution, collection and analysis of the outcomes survey.

04-16.13 • COMPUTER CRIMES & SOFTWARE PIRACY [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this Technology Policy and Procedure is to identify information and legislation governing computer crimes and software piracy (Florida Computer Crimes Act) and relate applicable requirements of the law (Chapter 815, Florida Statutes) to the College environment.

Description/Procedure:

The Florida Computer Crimes Act was passed into law in 1978 and was intended to address a growing number of computer-related crimes including acts against data, databases, hardware and computer systems, as well as software piracy. The provisions of the Act are as follows:

Florida Computer Crimes Act

1.2 Chapter 815, Florida Statutes

1.2.1 Fla. Stat. 815.01 Short Title

The provisions of this act shall be known and may be cited as the "Florida Computer Crimes Act."

1.2.2 Fla. Stat. 815.02 Legislative Intent

The Legislature finds and declares that:

- Computer-related crime is a growing problem in government as well as in the private sector.
- Computer-related crime occurs at great cost to the public since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white-collar crime.
- The opportunities for computer-related crimes in financial institutions, government programs, government records, and other business enterprises through the introduction of fraudulent records into a computer system, the unauthorized use of

computer facilities, the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets, are great.

- While various forms of computer crime might possibly be the subjects of criminal charges based on other provisions of law, it is appropriate and desirable that a supplemental and additional statute be provided which proscribes various forms of computer abuse.

1.2.3 Fla. Stat. 815.03 Definitions

As used in this chapter, unless the context clearly indicates otherwise:

- "Intellectual property" means data, including programs.
- "Computer program" means an ordered set of data representing coded instructions or statements that when executed by a computer; cause the computer to process data.
- "Computer" means an internally programmed, automatic device that performs data processing.
- "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.
- "Computer system" means a set of related, connected or unconnected computer equipment, devices, or computer software.
- "Computer network" means a set of related, remotely connected devices and communication facilities including more than one computer system with the capability to transmit data among them through communications facilities.
- "Computer system services" means providing a computer system or computer network to perform useful work.
- "Property" means anything of value as defined in S.812.011 and includes, but is not limited to, financial instruments, information including electronically produced data and computer software and programs in both machine- or human-readable form, and any other tangible or intangible item of value.

- "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security.
- "Access" means to approach, instruct, communicate with, store data, retrieve data, or otherwise make use of any resources of a computer, computer system, or computer network.

1.2.4 Fla. Stat. 815.04 Offenses against Intellectual Property

- Whoever willfully, knowingly, and without authorization modifies data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.
- Whoever willfully, knowingly, and without authorization destroys data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.
- Whoever willfully, knowingly, and without authorization discloses or takes data, programs, or supporting documentation which is a trade secret as defined in S. 812.081 or is confidential as provided by law residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property....
- Except as otherwise provided in this subsection, an offense against intellectual property is a felony of the third degree, punishable as provided in S.775.082, S. 775.083, or S.775.084.
- If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony in the second degree, punishable as provided in S.775.082, S.775.083, or S.775.084.

1.2.5 Fla. Stat. 815.05 Offenses against Computer Equipment or Supplies

...

- Whoever willfully, knowingly, and without authorization modifies equipment or supplies used or intended to be used in a computer, computer system, or computer network commits an offense against computer equipment or supplies.
- Except as provided in this paragraph an offense against computer equipment or supplies as provided in paragraph (a) is a misdemeanor of the first degree, punishable as provided in S.775.082, S.775.083 or S.775.084.

If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony in the third degree, punishable as provided in S.775.082, S.775.083, or S.775.084.

Whoever willfully, knowingly, and without authorization destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization destroys, injures, or damages any computer, computer system, or computer network commits an offense against computer equipment or supplies.

Except as provided in this paragraph an offense against computer equipment or supplies as provided in paragraph (a) is a misdemeanor of the first degree, punishable as provided in S.775.082, S.775.083, or S.775.084.

If the damage to such computer equipment or supplies or to the computer, computer system, or computer network is greater than $200 but less than $1,000, then the offender is guilty of a felony of the third degree, punishable as provided in S.775.082, S.775.083, or S.775.084.

If the damage to such computer equipment or supplies or to the computer, computer system, or computer network is $1,000 or greater, or if there is an interruption or impairment of governmental operation or public communication, transportation, or supply of water, gas, or other public service, then the offender is guilty of a felony of the second degree, punishable as provided in S.775.082, S.775.083, S.775.084.

1.2.6 Fla. Stat. 815.06 Offenses against Computer Users

Whoever willfully, knowingly, and without authorization access or causes to be accessed any computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another commits an offense against computer users.

...

Except as provided in this subsection an offense against computer users is a felony of the third degree, punishable as provided in S.775.082, S.775.083, or S.775.084.

If the offense is committed for the purposes of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony of the second degree, punishable as provided in S.775.082, S.775.083, or S.775.084.

1.2.7 Fla. Stat. 815.07 This Chapter is Not Exclusive

The provisions of this chapter shall not be construed to preclude the applicability of any other provision of the criminal law of this state, which presently applies or may in the future be applied to any transaction, which violates this chapter, unless such provision is inconsistent with the terms of this chapter.

1.2.8 Fla. Stat. 815.08

If any provision of this act or the application thereof to any person or circumstance is held invalid, it is the legislative intent that the invalidity shall not affect other provisions or applications of the act which can be given effect without the invalid provisions or applications, and to this end the provisions of this act are severable.

1.3 Summary of Fla. Stat. 755.082 and 755.083

Below is a summary of the penalties applicable to the offenses described in the act. Penalties for habitual offenders are dealt with in S.775.084, which is not included below.

1.3.1 Misdemeanor of the First Degree

Up to 1 year of imprisonment and a fine of up to $1,000 or any higher amount equal to double the pecuniary gain derived from the offense by the offender or double the pecuniary loss suffered by the victim.

1.3.2 Felony of the Second Degree

Up to 15 years of imprisonment and a fine of up to $10,000 or any higher amount equal to double the pecuniary gain derived from the offense by the offender or double the pecuniary loss suffered by the victim.

1.3.3 Felony of the Third Degree

Up to 5 years of imprisonment and a fine of up to $5,000 or any higher amount equal to double the pecuniary gain derived from the offense by the offender or double the pecuniary loss suffered by the victim.

Violations and Liability

Violator	Liable Parties
Student	Student violator, Supervisor of Student, Professor, Dean and/or Executive Dean, Campus President, Provost, President and Board of Trustees
Employee	Employee violator, Supervisor, Dean and/or Executive Dean, Campus President, Provost, President and Board of Trustees
Lab User/Visitor	Lab user/visitor violator, Access Provider, Lab Assistant, Micro Computer Technician, Integrated Systems Specialist, Campus Computer ApplicationsSpecialist, Network Application Specialist, System, Administrator, Dean and/orExecutive Dean, Campus President, President and Board of Trustees

Table 4.1: Violations and Liability

Case law holds that liability for software copyright violations does not require knowledge on the host's part. The host must be able to prove that they tried to prevent illegal software usage and have made all reasonable efforts to do so.

Reducing Liability

It is incumbent upon everyone within the College, Technology Division, and College Managers, to ensure due diligence is taken to assure compliance with applicable legal requirements and reduce the College's potential liability for violations.

Under the direction of the AVP, Educational Technology an annual assessment of compliance will be performed and recommendations for improvements will be made as necessary.

- Proactive Education

- Be proactive in providing copyright education for College employees.
- Post Signs
- Post signs showing the College's policy on copyrighting.
- Put in Licenses
- Have usage that written into software licenses when you purchase software so that you will not have to violate the license to get your job done.
- Class Curricula
- Include the College policy on software copyright in class syllabi.
- Handouts
- Distribute handouts to employees and students explaining copyright laws.
- Meetings
- Hold meetings within department to discuss ways to comply with software copyright.
- Know Licenses
- Know the contents of licenses for the software to in order to be familiar with what is legal.
- Signed Statements with Distribution
- Some departments may want to have employees or students sign statements, agreeing to abide by copyright law and license requirements, when they are given software to use.
- Policy (general) and Guidelines
- Ensure departments have a policy regarding software copyright and procedures for complying or make departments aware of the College's policies and procedures.
- Get Permission in Writing
- If there is a need to make additional use of a software product beyond that is in the license, get permission in writing from the vendor.
- Permission Notebook (licenses, POs, shareware receipts, permission)
- Keep a software notebook containing copies of licenses, POs, shareware receipts, and written permissions for software on the machines in the department.
- Do Software Audits by Hand or Use Auditing Software

Area	Requirement/Responsibility
Campus Learning Assistance	Learning Assistance Lab Manager; Microcomputer Technician
Centers	Integrated Systems Specialist; Campus Computer Applications Specialist
Campus Computer Labs	Computer Lab Manager; Microcomputer Technician; Integrated Systems Specialist; Campus Computer Applications Specialist
Program Specific Computer Labs	Program Faculty; Microcomputer Technician; Integrated Systems Specialist; Campus Computer Applications Specialist
Campus Computing Systems	Director of Administrative Services; Microcomputer Technician; Integrated Systems Specialist; Campus Computer Applications Specialist
Collegewide Network Systems	Associate Vice President, Technology Operations; Director of Networks and Communications
Collegewide Compliance	AVP, Education Technology

Table 4.2

The information contained within this TPM contains copyrighted material from the Software Publishers Association (SPA).

Software Publishers Association

1730 M Street Northwest

Suite #700

Washington, D.C. 20036

04-17.13 • TECHNOLOGY APPROVAL DUE DILIGENCE [RENNIE]

Recommended By: Robert J. (Rob) Rennie, Ph.D., VP, Technology & CIO

Purpose:

The purpose of this procedure is to describe the due diligence process of the technology division in the selection and approval of technology solutions. Reference 04-13 – Standard and Non-Standard Software Acquisitions for information pertaining to software acquisition and to provide documentation of the process to be followed in the acquisition cycle. Reference 04-14 – Hardware Acquisition for information as it pertains to standard and non-standard hardware acquisition Collegewide.

Description/Procedure:

**For the current process, reference the Technology Software Acquisition Requirements in the Employee Portal. Once logged in the document is found from top navigation link "Technology", then left navigation link "Technology Requirements."*

The technology division of the College is responsible for performing due diligence evaluations of technology solutions for the College. The College's CTO is specifically charged with ensuring the efficacy, appropriateness, cost effectiveness, and technology fit of potential solutions prior to approval for acquisition. Depending upon the size, scale, and scope of the solution, one of several processes may be employed.

For the purposes of due diligence in selection, the following definitions of technology solutions provide the foundation for method selection:

Software

Minor software is defined as software with an acquisition cost below $1,000 that is intended for stand-alone (non-server based, not requiring integration, not for broad distribution, and in compliance with Technology Requirements) use.

Major software is defined as any software product on any platform that does not meet the definition of minor.

The selection and acquisition requirements for software for these categories are published in the Technology Requirements document.

Services

The use of OPS agreements is subject to the College's APMs regarding cost limits, procedures, and approval authority.

Contracted service providers (programming, project management, database administration, network and systems management, etc.) are determined through one of the following methods: (1) RFP, RFQ, RFI, or competitive bid; (2) state contract; (3) other public entity's acceptable contract; and (4) specific vetting of service providers by Technology Department management.

Integrated Solutions

Integrated Solutions are defined as those where hardware, software, and/or services are combined to provide one solution offering. Integrated solutions are evaluated by Technology Department management and other appropriate stakeholders, based on the intended use of the solution, its breadth of intended deployment, technology capability and compatibility, useful life, and cost effectiveness.

Cloud Solutions

Cloud solutions are defined as subscriptions, platforms, software, and infrastructure-as-a-service (PaaS, SaaS, IaaS). The due diligence methodology applied to solutions in this category are as follows: research of available solutions, vetting of solutions providers, analyst and customer reference checks, evaluation of technology architecture, analysis of cost, assessment of integration requirements, and determination of value proposition (decision pack) for chosen solution.

Hardware

Hardware specifications are determined by analysis of available computing platforms including: architectural compatibility, performance specifications, operating system flexibility, relevancy, sustainability, consistency with college green computing initiative, life expectancy, and projected total cost of ownership. The results of this due diligence exercise are published in the College's Technology Requirements document and are reviewed quarterly and updated as necessary.

Summary

The College engages in a robust due diligence process for the selection and acquisition of technology solutions. This process is managed by the College's CTO who is charged with developing and monitoring adherence to the due diligence methodology. CIO and/or CTO approval of the selected process and solution must occur prior to acquisition. The College's CTO shall review, on a continual basis, technology solutions for their relevance and value to the College.

All acquisitions are made in conformance with the College's documented purchasing procedures.

05-01.13 • PROJECT MANAGEMENT DEFINITIONS [REIMAN]

Recommended By: Dennis Reiman, AVP, Tech, Associate CIO & CTO

Purpose:

The purpose of this section is to describe the requirements of project management for technology projects with varying size, scope, and cost.

Description/Procedure:

College technology projects are envisioned, planned, coordinated, and managed by team leaders who break each project into conquerable tasks. These are entered and managed with project management instruments that include, but are not limited to task management and selected calendars for project management (refer to 05-02 – Project Management Standards).

Task and project planning are used to better manage the use of resources (including purchases); plan for future needs, assess performance, evaluate effectiveness and deficiencies of resource utilization, analyze trends of service demands, review workload, and provide an accounting of resource utilization to clients and stakeholders.

05-02.13 • PROJECT MANAGEMENT STANDARDS [REIMAN]

Recommended By: Dennis Reiman, AVP, Tech, Associate CIO & CTO

Purpose:

The purpose of this section is to define the standards used in project management instruments (Microsoft Project, OmniPlan), resource availability/allocation tools (Microsoft Exchange, Microsoft SharePoint), and project knowledge base (Confluence, JIRA).

Description/Procedure:

The project numbering schema is alphanumeric. The first character is a letter. This letter is followed by a dash and two numbers (e.g. A-00 to A-99 or B-23). The letters and numbers progress in order and are used to assist with project control and reference.

New projects are approved and prioritized by Technology Division leadership and the respective team leaders. Project prioritization must be balanced and adjusted to account for routine tasks, short term demands, and critical interruptions. Projects are significant endeavors that require plans.

Two types of project plans are used. The overview level project plan must include the following details:

- Project Number
- Project Brand Name
- Project Synopsis
- Project Personnel
- Project Due Date & Milestones
- Primary Tasks
- Predecessors - Identified & Impact
- Conflicts
- Resource Requirements & Availability
- Decision (financial) Packet

- Comments

The Confluence platform is the repository for project plans. The detailed level project plans involve significant information and use project planning software (Microsoft Project, OmniPlan). These are working documents and reside with the functional lead on a project.

Both types of project plans should be updated regularly to ensure accuracy.

Task addition, modification, and deletion should be reflected in the project plan. Both external and internal delays should be documented. It is recommended that team leaders review the project plans regularly and make necessary updates.

Following project completion, an outcomes instrument (form/survey) should be provided to the primary client/customer to complete. The results should be reviewed and a service gap analysis should be performed (if applicable).

Functional Area	Functional Area Code	Sub Unit	Sub Unit Code
Academic Systems	3		
		Microsoft	1
		Unix	2
		Appliance	3
		Infrastructure	4
		Voice & Video	5
		Services	6
		General Supplies	7
Educational Technology	4		
Data Applications	6		
		Student Sub-systems	10
		Finance Sub-systems	20
		Financial Aid	30
		Per Payroll/HR Sub-Systems	40
		Miscellaneous	50
Multimedia Technologies	7		
		Digital Asset Management Team	1
		New Media Team	2
E-Systems	8		
		MIS Leadership	0
		E-Systems	10
		Data Management	30
Data Management	9		
Telecommunications	10		
CIO Office	11		
		Technology Division Operations	1

Functional Area	Functional Area Code	Sub Unit	Sub Unit Code
		Strategic Technology Plan	2
		Wave 3 Technologies	3
		Policies and Procedures	4
		Decision Packages	5
		IT Leadership Academy	6
Learning Innovations	13		
Educational Research	14		
		State Reporting	1
		Institutional Effectiveness	2
		QEP/Title III	3

Table 5.1: Project File Naming Standards

The next four (4) digits of the file naming is the project number. This is a non-duplicated number (incremental is the preferred method). The last two (2) digits of the fiscal year will represent the final two (2) digits.

The project files should utilize resources from the contact list. This will allow the projects to "share" resources and allow project participants to be alerted of tasks related to the projects they have been assigned. The calendar for the contact/resource selected should reflect the individual (team member) schedules for six (6) to eight (8) hour workdays. This value will depend on whether you're working a modified schedule (i.e. four 10s). This gap should reflect an average amount of daily time spent on E-mail, quick maintenance, helpdesk tickets, meetings, and project management. The resource calendar should also be kept up-to-date with holidays, planned vacations, and sick days. Keeping up to date with scheduling will ensure that estimated task/ project timelines would be quite accurate.

New projects are to be approved and prioritized by the team leaders. The area manager, director, or administrator may change prioritization of projects.

New project plans should be created for new projects that will take eight (8) or more hours of total team resources. Projects that will take less than eight (8) hours are to be created as a new project file or appended to a generic project plan for the team.

New project plans must include the following details:

a. Estimated project start date
b. Project owner (identify in the document properties)
c. Tasks
    1. Estimated duration - Estimated task duration should not exceed three (3) days. Break task into subtasks if this condition occurs.
    2. Predecessors (as required)
    3. Resources
        i. Internal – by name
        ii. External – by name or department

Daily tasks such as maintenance (to completed projects) should be documented in the original project plan (if one exists). Minor maintenance (i.e. takes a few minutes of resources) does not need to be documented since they are a part of the time gap provided in the contacts pool.

Project plans should be updated continuously to ensure accuracy. Task addition, modification, and deletion should be reflected in the project plan to reflect the project. Both external and internal delays should also be updated in the project plan notes. The notes field is an appropriate place to include a copy of an email or other correspondence (if it's an external delay). It's recommended that team leaders review the project plans nightly and make necessary updates.

Following project completion, an outcomes instrument (form/survey) should be provided to the primary client/customer to complete. These will also be kept on file with the project and may be used to perform a service gap analysis.

05-03.13 • APPLICABILITY & REQUIREMENTS OF PROJECT MANAGEMENT [REIMAN]

Recommended By: Dennis Reiman, AVP, Tech, Associate CIO & CTO

Purpose:

The purpose of this Technology Policy and Procedure is to provide information on the applicability and requirements of project management as used in the Technology Division.

Description/Procedure:

Information regarding the applicability and requirements of project management is defined extensively within 05-02 – Project Management Standards.

That information establishes a base system for managing projects. The applicability and requirements generate timelines and controls for good managerial practices. The result is a Technology Department that maintains a focus on and moves the primary vision, mission, and objectives of the institution to a higher level while balancing the day-to-day demands.

05-04.13 • FINANCIAL REPORTING BY PROJECT [THOMAS]

Recommended By: Kelly Thomas, Director, Technology Administration

Purpose:

The purpose of this Technology Policy and Procedure is to provide information on financial reporting by project within the Technology Department.

Description/Procedure:

The manner in which the Technology Department follows the budget and finance submission calendar and process, as well as the provision of individual project "project code(s)" is described within TPM 04-04.08 (Budget and Fiscal Analysis). The post-project analysis consists of identification of all expenditures associated with a specific "project code", which is then compared against the estimates defined in project plans or decision packages. The resulting analysis of operating costs or decision package provides for monitoring, evaluation of objective achievement, and continuous quality improvement of technology projects.

06-01.13 • DEFINITION [REIMAN]

Recommended By: Dennis Reiman, AVP, Tech, Associate CIO & CTO

Purpose:

The purpose of this section is to describe the functions and technical environment of E-Systems Technology.

Description/Procedure:

E-Systems Technology is responsible for advanced web development and enterprise systems integration in the support of College goals and initiatives. The Microsoft .NET Framework and Java Technology represent the current sets of standards and practices for all e-systems, e-commerce, and web-related development.

The .NET framework implementation focuses on web services (XML data exchange) enablement with a web interface. The framework supports the development and integration of secure web services (using encryption and/or authentication) for data retrieval. Application classes have been developed to integrate with the enterprise system (ORION) using Software AG's webMethods EntireX. The Service Oriented Architecture (SOA) model allows seamless integration into other system environments and applications. This includes integration with the courseware/e-learning systems (e.g. Blackboard, Canvas). Additionally, SOA allows seamless integration with Java-based components, Business Process Management (BPM), Enterprise Communications (Microsoft Exchange) and with reporting solutions.

The Artemis/Connections web portal provides single point of entry for all transactions including schedule search, transcripts, registration, payment (including credit card), financial aid, grade reporting- input and viewing, instructor and personal schedules, grading performance and distribution analysis, class rosters, paid vs. unpaid enrollment, program of study evaluation, degree planner, profile maintenance and personal information update, open class search, on-line college catalog, mileage reimbursement, web-based reporting, etc. By basing this development on web services, this application is accessible through many different types of digital devices (including desktop web browsers and mobile devices).

E-Systems Technology includes two distinct groups: E-Systems Development and Integration and Multimedia Design (refer to 06-02 – Structure).

06-02.13 • STRUCTURE [REIMAN]

Recommended By: Dennis Reiman, AVP, Tech, Associate CIO & CTO

Purpose:

The purpose of this section is to describe the functions and responsibilities of the teams within E-Systems Technology.

Description/Procedure:

The Development and Enterprise Application Integration Team is responsible for all Collegewide e-systems structural design, coding, testing, and implementation and the provision of high-level programming support for all areas of the Technology organization of the College. This team provides advanced language scripting in support of various projects as well as ERP/B2B integration and portal development and maintenance.

- Specific responsibilities of the E-Systems Development and Enterprise Application Integration group include:
- Web Application Development and Support
- Student and Employee Portal Development and Support
- Systems Integration for systems within the Florida State College at Jacksonville Comprehensive Technology Vision.

Multimedia Authoring

- The Multimedia Authoring Team is responsible for the design, development and implementation of multimedia content in support of College technology initiatives and projects. The team provides advanced authoring of multimedia content for E-Systems projects.
- Specific responsibilities include, but are not limited to:
- Develops web-based content
- Provides rich client interface design
- Evaluates multimedia development tools
- Provides support to E-Systems Integration team for the development of software products

06-03.13 • METHODOLOGY [REIMAN]

Recommended By: Dennis Reiman, AVP, Tech, Associate CIO & CTO

Purpose:

The purpose of this section is to describe the development methodology used by E-Systems Technology.

Description/Procedure:

E-Systems Technology utilizes the eXtreme Programming (XP) methodology for the planning, designing, coding, and testing of web applications. Refer to 10-05 – Reference Standards - eXtreme Programming.

06-04.13 • DEVELOPMENT [REIMAN]

Recommended By: Dennis Reiman, AVP, Tech, Associate CIO & CTO

Purpose:

The purpose of this section is to describe the development processes of E-Systems Technology.

Description/Procedure:

Requests for new development projects (applications and enhancements) must be submitted through the Artemis Employee Portal using the IT Request System (refer to 13-04 – Service Request Process). Additionally, requests for bug fixes in existing applications to be submitted through the IT Request System, and will be evaluated and addressed upon receipt.

The Lead E-Systems Developer is responsible for the development and maintenance of the project plan(s) using the approved project management instrument (refer to 05-02 – Project Management Standards).

Project acceptance is established by the Lead E-System Developer with the approval of the Director, Information Systems (E-Systems) based on an analysis of project need (net-benefit), size, scope, and cost. IT Requests for new development or project enhancements that will require a development effort longer than three (3) days will be prioritized by the ORION/Connections Executive Committee. Application user groups can establish the priorities within their project list maintained by the governance.

Project development must occur on a test server to ensure that the production system is not affected by the development (refer to 06-05 – Testing).

06-05.13 • TESTING [REIMAN]

Recommended By: Dennis Reiman, AVP, Tech, Associate CIO & CTO

Purpose:

The purpose of this section is to describe the testing methodology used by E-Systems Technology.

Description/Procedure:

E-Systems Technology utilizes the eXtreme Programming (XP) methodology for the planning, designing, coding, and testing of web applications. Refer to 10-05 – Reference Standards - eXtreme Programming.

06-06.13 • PRODUCTION [REIMAN]

Recommended By: Dennis Reiman, AVP, Tech, Associate CIO & CTO

Purpose:

The purpose of this section is to describe the procedures for the testing and migration of applications developed by E-Systems Technology into the production environment.

Description/Procedure:

The purpose of this section is to describe the procedures for the testing and migration of applications developed by E-Systems Technology into the production environment.

Description/Procedure:

New applications/releases/upgrades must be developed and tested in a test environment (refer to 06-05 – Testing). If applicable, user group managers/directors must provide sign-off prior to release into a production environment.

Hot fixes (emergency corrections) to the system are to be migrated into production at the discretion of the Lead E-Systems developer. If downtime is required for the migration of the hot fix, the appropriate (and applicable) groups/individuals will be notified regarding the problem from the contact list (see example below).

The release of new/modified applications is handled through Visual Source Safe (refer to06-08 – Library Management and Change Control8).

The migration of data to the production environment must also be planned and coordinated with the release of corresponding applications.

The Lead E-Systems Developer and identified delegate are responsible for the migration of programs and data into the production environment. Following the migration of new applications or enhancements, the system must be thoroughly tested to ensure system integrity and validity.

Contact List

- Director, E-Systems
- Director, Application Systems

- Database Administrators
- E-Systems Team members
- User groups (managers)
- Technical Help Desk

06-07.13 • PROGRAMMING STANDARDS [REIMAN]

Recommended By: Dennis Reiman, AVP, Tech, Associate CIO & CTO

Purpose:

The purpose of this document is to provide a standard for development of program code. The aim of the standard is to make code readable and simple to maintain.

Description/Procedure:

Naming Conventions

- Identifiers should be given language-independent, meaningful names. See Code Complete, Second Edition (McConnell, 2004), section 10.2.
- Hungarian notation will be used to declare identifier names.
- Minimize scope when possible.
- Variables will be typed when declared. (Very few exceptions)
- Names should not conflict with library-routine names or pre-defined variable names.

Comments

- Commenting can be a valuable and time saving technique when done properly.
- Comments should be written explaining ‘why’ instead of ‘how’. Comments should make statements about the code that the code itself cannot.
- Comments should not emulate the code.
- Header comment will contain, at a minimum:
  - •Author
  - •Original Date
  - •Purpose
  - •Modification History
  - •Comments that are added by a programmer other than the one listed in the header comment section should contain the user ID and date.
  - •Example: “This block of code was modified mm/dd/yy. <userID>”

- Additional commenting standards are presented in Code Complete, Second Edition, sections 32.3, 32.4 and 32.5.

Documentation

See Technology Policies and Procedure Manual 06-09 – Documentation.

Error Handling

- Programmers will carefully check code for possible errors.
- Test cases will be developed that are thorough and unassuming. Test cases will be executed with the appropriate client group.

Error Handling (continued)

- Keep test cases and documentation for each test case. This information will be filed electronically in the e-system documentation area for each application developed.
- Errors will be repaired and released in accordance with the standards for the operating environment. Refer to Technology Policies and Procedures Manual 06-04 – Development, 06-05 – Testing, and 06-06 – Production.

Languages

- ASP.NET
- Visual Basic.NET (version based on released application environment)
- AJAX
- C#.NET (version based on released application environment)
- Java/Javascript
- Objective-C

Case

When writing code with a case insensitive programming language, the Visual Studio Integrated Development Environment and/or the Eclipse Development Environment will guide case.

Format and Layout

Formatting and layout for code written with this standard will follow layout guidelines presented in Code Complete, Second Edition (McConnell, 2004), Section 18, Layout and Style.

Browsers

- Code should be written for cross-browser/cross-platform compatibility.
- Code should be tested across the latest mainstream web browsers.
- Do not write code for browsers that are in Beta release.

Code Maintenance

Code maintenance will be conducted when necessary. Visual Source Safe (transitioning to Team Foundation Server in 2013) will be used as specified in the Technology Policies and Procedure Manual, 06-08 – Library Management and Change Control.

Quality Assurance

- The Lead E-Systems Developer will conduct code reviews during the testing phase of a programming project.
- Inspections of code will be conducted in accordance with Code Complete, Second Edition (McConnell, 2004), and Section 21.3.

References

McConnell, S. (2004). *Code Complete* (2nd ed.). Redmond, Washington: Microsoft Press.

06-08.13 • LIBRARY MANAGEMENT AND CHANGE CONTROL [REIMAN]

Recommended By: Dennis Reiman, AVP, Tech, Associate CIO & CTO

Purpose:

The purpose of this section is to describe the standards and procedures for library management and change control of developed code and documentation by E-Systems and other approved areas.

Description/Procedure:

E-Systems development must be accomplished using a library management and change control application. Visual Source Safe [transitioning to Team Foundation Server (TFS) in 2013] provides this capability and allows the E-Systems Team to efficiently manage application migration to production environment (refer to 06-06 – Production). The application provides version control preventing accidental file (code/documentation) loss; allow back tracking to previous versions; audit trail capabilities; and management of developed application/system release.

All projects (development code, documentation, etc.) must be stored in the Visual Source Safe/ TFS database. Application and system security ensures that only the members of the E-Systems Team, and additional approved individuals, have access to all of the code and documentation. The application database should be backed up on a nightly basis to ensure that should a "disaster recovery" situation occur, only limited loss of development time would be experienced.

Below is a list of the policies and procedures for utilizing the Visual Source Safe/TFS system.

- Code checked in must be in working condition (i.e. compiles without errors).
- Always label checked in items when getting the latest version of code and placing it on the development server.
- Specific code will only be migrated to the production environment following a satisfactory version control report.
- Development builds must be performed on a regular basis.
- The version control database must be backed up on a nightly basis.

Code/documents must be stored in the Visual Source Safe/TFS database and be available to all developers of the E-Systems Team.

06-09.13 • DOCUMENTATION [REIMAN]

Recommended By: Dennis Reiman, AVP, Tech, Associate CIO & CTO

Purpose:

To provide procedures for documenting the design, development, and implementation of web based applications by the E-Systems group. These procedures may also apply to stand-alone applications.

Description/Procedure:

Documentation of an application should include at a minimum, but not limited to, the following:

- IT Services Request (JIRA)
- Project Plan built using approved toolset (05-02 – Project Management Standards)
- Design Document/Storyboard (JIRA)
- Source Code in Repository [Source Safe/Team Foundation Server (2013 transition)]
- Testing (JIRA)
- Sign-off (JIRA)
- Change History (JIRA)
- Release History (transitioning to Confluence in 2013)
- Application Downtime Report (transitioning to Confluence in 2013)

All documentation shall be stored in accordance with Technology Policies and Procedures Manual, 06-08 – Library and Change Management Control.

07-01.13 • DEFINITION [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to define the functions and responsibilities of Application Systems.

Description/Procedure:

Application Systems is responsible for providing maintenance and support of the College-wide enterprise resource planning system, know as ORION. Personnel within the Applications Systems team provide development and maintenance services for all ORION modules servicing the student community and administrative services (HR, Finance, etc.).

07-02.13 • CHANGE CONTROL [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to provide a set of sequence steps that should be followed to ensure that jobs are moved successfully from the development environment to the intended destination.

Description/Procedure:

In order for developers to have modules/jobs moved from the development environment to acceptance or production, a written migration request via e-mail must be submitted to the Director of Information Systems (Applications), delegate reviewer, or Database Administrator (DBA). The developer must specify if the request is standard or an emergency. Upon receiving the request, the Director of Information Systems (Applications) delegate reviewer, or DBA shall determine if the Reviewer information is listed and shall then process the request within seventy-two (72) hours. If the request is an emergency, the request will be processed immediately. Upon completion of the migration the Director Information Systems (Applications) delegate reviewer, or DBA shall notify the developer and reviewer(s) via e-mail.

07-03.13 • PRODUCTION SCHEDULING [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to describe the process required to incorporate a batch job into the daily production schedule. This procedure enables Data Operations to ensure that all production jobs are executed according to the daily production schedule.

Description/Procedure:

The daily production schedule is created, updated and maintained by Data Operations. In order to have a job executed, a formal request must be submitted to Data Operations in the form of a faxed parm sheet or e-mail. It is the responsibility of the requestor to specify all of the necessary parameter information. Data Operations will not be held responsible for incorrect processing due to incorrect or missing parameter information.

07-04.13 • LIBRARY MANAGEMENT [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to describe the procedures associated with managing the data libraries within the Data Systems area, which is a comprehensive system to control and check the access to the NATURAL environment.

Description/Procedure:

The Information Technology Department has developed a system whereby there is restricted access to natural libraries. If an employee needs access to a natural library, that individual shall submit a request in writing to the Director of Information Systems (Applications). The request must specify the library involved, the reason access is needed and the time frame for which access is required. After receiving the aforementioned information, the Director of Information Systems (Applications) shall grant or deny the request. If the request is granted, the Director of Information Systems (Applications) will forward the original request to the Database Administrator (DBA) who will then process the request within the specified time frame. The procedure is required to protect the NATURAL environment against unauthorized access and improper use.

07-05.13 • CHANGE MANAGEMENT STANDARDS [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to describe the procedures associated with controlling access to production modules.

Description/Procedure:

Information Technology has implemented DBMS standards designed to prohibit developers from modifying programs in acceptance or production. If developers need to change a production module, a copy of the module should be retrieved and modifications should be made in the test environment (P&P 07-16 – Peer Review shall be followed).

Developers are not allowed to implement modules from test or acceptance to the production environment. In order to have a module moved to the production environment, the developer must provide the DBA a written request, specifying the name of the module and the time frame for which the module is needed in production. Except for immediate-priority requests to resolve production problems, there will be a three (3) day delay in all standard production requests. Batch production jobs should only be executed from appropriate libraries in the production environment.

07-06.13 • OPERATING ENVIRONMENT [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to describe the College's enterprise system operating environment.

Description/Procedure:

Florida State College at Jacksonville performs its enterprise system (ORION) processing on an Oracle Enterprise Server. The server connects to SAN storage, as well as an Oracle backup system. The current Operating System is Sun Solaris.

This Oracle Enterprise Server houses the College's mission critical and archival data, and is an integral part of many applications, including the web-enabled student and employee portals. The Oracle Enterprise Server, in concert with a Microsoft SharePoint based front-end application (Artemis), comprise Florida State College's enterprise resource planning (ERP) system.

Beyond the Solaris operating system, the enterprise system utilizes Software AG's Natural, a 4GL programming language, designed for building mission-critical applications. For the system's database needs, Software AG's Adabas is utilized, along with webMethods EntireX/ Integration Server, integration software that allows legacy systems such as ORION to feed data to web enabled applications for e-commerce. Finally, the application development and interoperability area is aided through the use of Natural Construct, a model-based application generator used for reducing development time.

07-07.13 • BATCH EXECUTION/UNIX SCRIPTS [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to provide a set of sequence steps that should be followed to create UNIX Scripts for batch job execution.

Description/Procedure:

The first step in creating UNIX Scripts is to include the appropriate standard copycode already available for job-step indication. Proper work files will be identified and named according to Batch Documentation provided as an ORION deliverable. A test run of the Script is executed in both the Test and Acceptance environments. If the test is successful, the Script is migrated to the Production environment at time of implementation. However, prior to executing the Script in the Test, Acceptance or Production environment, all documentation must be completed in the Batch Submittal System, which is basically a system where all jobs are defined and allows end-users to execute production jobs.

Steps involved in creating UNIX scripts include following appropriate scripting standards and programming logic. Create a backup of original file for existing scripts that are modified. Use the correct syntax to declare which shell the script will call. Include author name when creating or modifying script and include date. Comments should be included to explain the script commands and changes. Comments should include the purpose of the script. Layout must be clear and readable. Unnecessary commands should be avoided to improve efficiency of script. Before executing a new or modified script in production, the script must execute successfully in the test and development environment if applicable.

07-08.13 • SYSTEM PROGRAMMING SERVICES & SUPPORT PROCESS [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to describe the College's Systems Programming Services & Support Process.

Description/Procedure:

The current operating system (OS) for the College's enterprise system is Sun Solaris. The maintenance and functionality of the OS is the responsibility of the Open Systems Team.

The Open Systems Team leader will manage the systems programming functionality including determining priorities and requirements.

07-09.13 • DEVELOPMENT [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to provide procedures to be followed by user departments in requesting research, program modifications or new programs.

Description/Procedure:

All IT Service Requests must be submitted to the Directors of Information Systems (Applications & E-systems) via the College's formal Request system (JIRA) available through the Employee Portal. The Directors will review the requests not indicated as emergencies to determine those which need to be flagged as institutional priorities. These are items that result in a developers time exceeding a forty (40) hour workload and will be taken to the ORION/ Connections Executive Committee for prioritization.

Emergency Requests: These are defined as items requiring IMMEDIATE attention with a 24 hour turn around.

All items that are required to maintain the integrity of the business will receive higher priority. These activities include problem research and resolution, environment changes, and performance enhancements. In summary, these activities are necessary in order for us to function as an educational institution and would adversely impact the manner in which we conduct business if not implemented.

Discretionary items are items that are not absolutely necessary, but are preferred by end-users. These will receive a lower priority unless the request result into an NEW PROJECT and the Executive Committee assigns a higher institutional priority.

Any exceptions will require the approval of the requester's Cabinet level administrator and the College VP for Technology or Executive Director, Enterprise Applications.

07-10.13 • ACCEPTANCE ENVIRONMENTS IN ORION [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to describe the type of access developers have to the Acceptance Environment in ORION. This procedure enables the College to protect the Acceptance Environment against unauthorized access and improper use.

Description/Procedure:

The Database Administrator (DBA) grants access to the Acceptance Environment. Access granted is solely for the pursuit of activities related directly to the mission of the college. The only access granted to this environment includes the ability to view libraries. Programmers are not authorized to update in any way (i.e. catalog, save, delete, update). In addition, programmers are not permitted to move programs to acceptance; that is done by the DBA, delegate reviewer, or Director Information Systems (Applications) only.

07-11.13 • PRODUCTION ENVIRONMENT IN ORION [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to describe the type of access developers have to the Production Environment. This procedure enables the College to protect the Production Environment against unauthorized access and improper use.

Description/Procedure:

The Database Administrator (DBA) grants access to the Production Environment. Access granted is solely for the pursuit of activities related directly to the mission of the college. The only access granted to these environments includes the ability to view libraries. Programmers are unauthorized to update in any way (i.e. catalog, save, delete, update). In addition, programmers are not permitted to move programs to production; that is done by the DBA only.

07-12.13 • ORION/ARTEMIS GOVERNANCE STRUCTURE [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to define the roles and responsibilities of ORION/Artemis Executive Committee.

Description/Procedure:

ORION/Artemis Executive Committee

This committee is chaired by a member of the cabinet and includes representation from College user groups and faculty.

General Purpose

- To determine, approve, and direct priority requests from user and technology communities.
- Identify representation on State/Federal Departments and Legislative levels to determine requirements for compliance.
- Identify requirements at Florida State College at Jacksonville to provide better solutions/ service.
- Determine reporting procedures and structure for all IT-Service Requests

Committee Members

The Committee members are individuals who envision the project and attract others to both assist and take on additional leadership as the systems mature.

Currently, there are seven user areas, which include the following:

- Faculty
- Facilities
- Financial Aid
- Finance/Credit and Collections
- Student

- Purchasing
- Human Resource (HR)

Each of these areas will have one (1) vote at Committee meetings for project prioritization. Meetings are held at least once per quarter. Areas not represented at the meetings will forfeit voting rights for the meeting.

07-13.13 • DOCUMENTATION FOR DATA OPERATIONS CENTER [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this section is to describe how documentation is developed and updated for new and existing processes for the Data Operations Center.

Description/Procedure:

In order for data operators to execute jobs in the Data Operations Center, every process will be properly documented as soon as it is implemented. Such documentation will include the proper instructions, times in which jobs started and ended and any relevant notes. All documentation will be filed in the Technology Operations area and kept readily accessible.

07-14.13 • SERVICE LEVEL AGREEMENTS [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

Priority	Issue	Contact	Resolution
1	Issue of the highest importance—mission-critical systems with a direct impact on the organization (Examples: widespread network outage, ORION/Artemis system, e-mail system, telecom system, delivery of instruction, etc.)	Immediate – 15 minutes	ASAP 4 hour response support on hardware issues by vendor
2	Group outage that is preventing the affected users from working (Examples: local network issues, network printing, etc.)	1 week	2 weeks - the maximum possible notification
3	Scheduled work (Examples: new network or server installation, new equipment/software order,)	1 week	2 weeks – the maximum possible notification
4	Single user outage that is preventing the affected user from working (Examples: failed hard drive, broken monitor, continuous OS lockups, etc.)	Each Campus to define appropriate time	Each Campus to define appropriate time
5	Single user or group outage that can be permanently or temporarily solved with a workaround (Examples: malfunctioning printer, PDA synchronization problem, PC sound problem, etc.)	Each Campus to define appropriate time	Each Campus to define appropriate time
6	Nonessential scheduled work (Examples: office moves, telephone moves, equipment loaners, scheduled events)	Each Campus to define appropriate time	Each Campus to define appropriate time

Table 7.1: Service Level Issues, Contacts and Resolutions

The purpose of this section is to outline the procedures associated with generating the Service Level Agreements between Technology Department and its Florida State College at Jacksonville clients.

Description/Procedure:

The Technology Department has developed a series of Service Level Agreements (SLA) to outline the required procedures for specific functions. Each SLA will be developed in conjunction with representation from each functional area to ensure expectations are met. SLAs will be updated by the Technology Department as needed.

Service Level Agreement (SLA)

Under normal operations, support will be given on a first-come, first-served basis and problems will be solved as soon as possible. However, the following ranking scheme should be used to categorize all requests for assistance. The contact and resolution times given below are the Technology Department's general guidelines under normal circumstances. During extraordinary situations, such as a natural disaster, prolonged power outage, or other catastrophic events, contact and resolution times may be longer. Items 3-6 below are Campus issues and are listed as guidelines for Campus support.

07-15.13 • SYSTEMS PROGRAMMING [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

Purpose of this section is to describe the support for the College's Enterprise Application Server system.

Description/Procedure:

The current operating system for the college's enterprise system is Solaris Unix. The maintenance and functionality of the operating system is the responsibility of the Open Systems Team. Hardware support is contracted to Oracle/Sun Microsystems, Inc. or their approved vendors. Due to the mission critical nature of this system, hardware support will be maintained at the highest available level.

07-16.13 • PEER REVIEW [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to describe the procedures to be followed by application programmers after making programming modification to existing applications or coding new programs and /or complete new systems.

Description/Procedure:

All programming changes to existing applications or coding of new programs and/or systems must undergo a code inspection prior to production implementation. A code inspection should consist of the following individuals:

Reviewer(s): Responsible for reviewing the programming modifications prior to migration request.

Programmer: Responsible for scheduling the code inspection review. The Programmer is responsible for selecting the Reviewer(s).

After the code inspection review process has been completed, the Reviewer(s) will inform the Programmer of the final disposition that will be of the following:

- **Accept:** the Reviewer(s) found the programming changes acceptable. No additional programming changes are needed.
- **Conditionally Accept:** Meaning the programming changes were conditionally accepted based on minor changes being made and reviewed by the Reviewer(s).
- **Re-inspect:** The programming changes were not acceptable. Programmer must make additional programming changes and reschedule another code inspection review.

NOTE: Following successful code inspection review, the programmer shall submit the electronic migration request form via e-mail to the Director of Information Systems (Applications) carbon-copying ("cc") the Reviewer(s). The issue code as assigned via the IT Request System will be used as name for the migration form and will be attached to the IT Request System. The Director of Information Systems (Applications) or delegate reviewer shall do the migration to the Acceptance environment and inform the programmer to continue with USER ACCEPTANCE TESTING. After User Acceptance Testing, (the reporting user performed a client sign off via the IT Request System) the assigned developer will forward the migration request to the Database Administrator (DBA) for migration to the production environment and update the IT Request System.

07-17.13 • SEPARATION OF DUTIES [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this Technology Policy and Procedure is to describe the natural separation of duties between Applications, Systems Programming, Database Administrator (DBA) and Operations.

Description/Procedure:

Applications:

The Applications area is responsible for handling the day-to-day requests from end users to ensure that Florida State College at Jacksonville business processes are not interrupted. Application Systems is responsible for making all programming changes to production modules. The Applications area should not make any changes to production files and/or databases. Any database/file changes should be requested from the DBA.

Systems Programming/Application Support:

Systems programming and application support are provided by the Open Systems Team that reports to the Executive Director, Enterprise Applications. Support is provided during normal hours of operation unless there is an emergency that requires support beyond normal hours of operation. The primary responsibilities of the Open Systems Team include installation and routine application maintenance, problem resolution and performance tuning of the base operating system, SAN storage subsystem, and necessary third party software products. Responsibilities also include monitoring systems during peak usage periods, providing immediate problem definition and resolution, as well as identifying ways to improve the operational process.

DBA:

The DBA is responsible for managing and ensuring the integrity of the databases in the Test, Acceptance and Production environment. The DBA should not modify any applications (production modules).

Operations:

Responsible for monitoring the performance and availability of systems, preparing documentation for various departments, ensuring backups for the system, executing and monitoring batch jobs, ERP reports, working with Applications and DBAs in optimizing and upgrading the ERP system, and notifying the appropriate personnel when there is a system interruption. Operations will NOT modify any databases or "in-house" developed applications (production modules).

07-18.13 • ERP/ORION II [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to describe the College's Enterprise Resource Planning (ERP) system.

Description/Procedure:

Florida State College at Jacksonville utilizes an ERP system, known as ORION II at Florida State College at Jacksonville. This solution provides automated utility across various functional areas, including:

- Credit & Collections
- Payroll
- Human Resources
- Financial Aid
- Accounts Payable
- Purchasing
- Finance
- Budget
- Student
- Facilities

ORION II is written in Natural, a 4GL programming language, with its associated database, ADABAS. A staff of programmer analysts (Engineer II & III Software), database administrators, and systems programmers (Engineer IV Software) supports the system and environment. The ORION/E-Systems Executive Committee defines priorities for development by the Applications Team for issues designated as projects.

The Director of Information Systems (Applications) is primarily responsible for supporting ORION II, ensuring availability and functionality as defined in appropriate service level agreements (SLA).

07-19.13 • SOLUTION ENVIRONMENT [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to describe the products used to support the Database Administrators (DBAs) and System Analysts in the Applications group.

Description/Procedure:

The Data Systems Solution Environment is comprised of the following Products:

Name of Product	Brief Description
NATURAL	Programming language used by System Analysts and Programmers
NaturalOne	Windows based programming and debugging
ADABAS	Database
SQL Gateway	Data Replication
PREDICT	Data Dictionary used to identify file changes
DBA Workbench	Adabas Related Services
UNIX Scripts	Used for submitting “batch” jobs
NATURAL SECURITY SYSTEM	Comprehensive system to control and check the access to our NATURAL environment

Table 7.2: Data Systems Solution Environment Products

07-20.13 • EXTERNAL DATA EXTRACT REQUESTS [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to describe the procedures associated with providing access to raw data.

Description/Procedure:

Permission and the necessary security requirements for the requestor must be verified with the data owner. Data owners are determined by the state as record keepers.

Access to data will be restricted to ORION system areas allowed by the data owner.

The requested data format will be evaluated and corrected if needed to fulfill security and interoperability requirements.

The appropriate methods for data communication will be determined based on data classification and volume. All parties involved will collaborate to determine data usage and training requirements. Support will be provided when needed.

The requested frequency will be reviewed to assess production system impact. A mutually accepted schedule will be adopted.

Sensitive data (personally identifiable information) shall not be stored on portable storage devices (e.g. laptops, palm pilots, thumb drives, etc.) or in personal cloud based storage (Dropbox, etc.).

The requestor will be fully accountable for complying with Federal, State, and College policies in the management of College Data.

08-01.13 • PHYSICAL ENVIRONMENT [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The intent of this section is to describe the characteristics associated with Information Technology physical computing environment at the Data and Network Operations Center.

Description/Procedure:

It is the policy of the College to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

- Physical Environment Management
- Physical access is controlled and logged through the facility's electronic security system and is limited to IT management and technical personnel required to perform job functions
- Rack mounted computer systems
- Wire management systems
- Raised floors
- Fire detection and suppression systems
- Conditioned uninterruptible power supply
- HVAC
- Automated monitoring of Data Center physical environment

08-02.13 • NETWORK SERVER SYSTEM (SERVER ADMINISTRATION) [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this section is to outline the procedure for the deployment and management of server systems on Florida State College at Jacksonville production networks.

Description/Procedure:

Server Administrator Duties

- Maintains system availability to users through daily monitoring.
- Provides application guidance, parameters and specifications to consultants in developing customized reports necessary to meet business needs including identifying data sources and structures.
- Develops and provides set-up specifications and parameters in the development of interfaces and other automated processes.
- Develops specifications for system modifications, corrections and testing of system changes prior to implementation.
- Coordinates the installation of new software, software updates, new hardware, etc.
- Communicates with users regarding current and prospective system changes and future needs.
- Plans, organizes, controls and maintains the scheduling of reports, interfaces, project logs and records, problem logs and progress of projects in relation to established time schedules and work outlines.
- Attends and conducts system planning, status and functional meetings.
- Serves as technical liaison with outside consultants and technical support staff.
- Performs system backup and restore procedures.
- Performs preventive and corrective maintenance and works with third party vendor technical support in timely resolution of issues.
- Analyzes and corrects data growth and performance issues.

- Provides system security administration in maintaining applicable operating system and application patches, adding and removing users, resolving access problems and determining level of system access.
- Places all Servers and Desktop Computers in Domains and Workgroups approved, and provides the correct naming convention determined by the Director of Networks and Telecommunications, with access granted to members of the Enterprise Systems Team. Example: dwc-staffid for staff and dwc-room#-# for classrooms.
- Performs related duties as assigned.

Physical Location of Server Systems

Server systems should be located only in areas approved by the Associate Vice President of Technology Operations.

Classroom maintained servers are to be kept off of the production network and remain within the test environment specified by the Associate Vice President of Technology Operations at all times.

Server housing locations should exhibit the following characteristics:

- Unless approved by the Associate Vice President of IT – Technology Operations, Enterprise Wide Services and Services provided to the Internet must be physically located at the Network Operations Center.
- Heightened physical access controls that allow access only to designated server administrators and other authorized personnel.
- Dedicated environmental controls for HVAC with automated failure notification.
- Uninterruptible Power Systems (UPS) that will provide line filtering and automated and unattended server shutdown in the event of an extended power outage.

08-03.13 • OPERATIONAL RANGE [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The intent of this section is to describe the Information Technology Department's operational range for the Data and Network Operations Center.

Description/Procedure:

The College utilizes dedicated high volume air conditioning (HVAC) and uninterruptible power supply (UPS) systems to maintain appropriate environmental conditions in the Data and Network Operations Center computer rooms. These systems maintain proper temperature, humidity and input power to all equipment. Target environmental operational parameters are as follows:

Temperature: 72 degrees Fahrenheit

Humidity: 50% relative humidity

Power: via UPS; AC only; filtered, 3-phase, 60 Hz, 110 and 220 volt

08-04.13 • FACILITIES SUPPORT [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The intent of this section is to describe the facilities support for the Information Technology Department's Data and Network Operations Center.

Description/Procedure:

Facilities support for the Data and Network Operations Center is provided by Facilities Department personnel employed by the College at the Deerwood Center and by third-party vendors as required. The Deerwood Center Facilities Department is the point of contact for facilities support issues unless otherwise noted. Detailed contact information is posted on HVAC and UPS equipment.

08-05.13 • FLORIDA STATE COLLEGE PEER-TO-PEER FILE SHARING [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this Policy and Procedure is to outline the peer-to-peer file sharing solution for Florida State College's computing environment.

Description:

Florida State College at Jacksonville utilizes a standalone Internet content filtering server appliance that is used to filter inappropriate material for students. The appliance also features filtering for peer-to-peer file sharing and illegal download. This service works in compliance with the American Council on Education (ACE) and the Recording Industry Association of America (RIAA).

In addition to peer-to-peer file sharing, Cabinet members may request other services to be filtered. While no content filtering method is completely 100% effective, Florida State College's Technology Department will provide the best effort possible to prevent access to inappropriate file sharing and downloads.

Filtering of peer-to-peer file sharing will be done throughout Florida State College's network infrastructure.

The content filter server appliance determines blocked sites and services in various ways such as regular library updates from the vendor, manual entry, and keyword entry.

When a person attempts to download the peer-to-peer file sharing application from its respective website, the site will be blocked. If the application is already installed on a computer and attempts to share or download content, the service will not traverse out of Florida State College's network and will be blocked from exiting the firewall.

When a person attempts to access a file-sharing site, they will be redirected to a block page listing the reason why the site was blocked. Because some legitimate sites may mistakenly get blocked, the redirected site also allows the student to initiate a request to the Technology Department to review the site and remove it from the library of blocked sites.

09-01.13 • PHYSICAL ACCESS TO THE NOC [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this section is to describe the process and procedures for managing physical access to the College's Network Operations Center (NOC) at the Deerwood Center.

Description/Procedure:

The Florida State College at Jacksonville NOC located in the Deerwood Center houses the Sun F12K, computer operations, server farm, and the applications and network staff. As the central hub for the College's Enterprise Resource Planning (ERP) system, ORION, Collegewide network (intranet) and associated servers, Internet, and the distance learning support platform, it is imperative to have sufficient physical access safeguards implemented.

The NOC is a stand-alone facility accessible 24 hours a day, 365 days a year. Proximity card locks control all three entrances into the facility (one external and two internal). To gain access through the electronically locked access points, an individual must possess a working access card issued by Director, Technology Administration. When the card is brought within sufficient proximity to the electronic lock, the door lock is released and an appropriate online annotation of the access is recorded in system's database.

The following procedures are germane:

> The Director, Technology Administration approves issuance and access level of all access cards for the NOC. General access to the NOC is provided to approved IT personnel. Access to the computer floor is limited to computer operators, the Operations Manager, and senior IT managers at the AVP level and above. Access to the server farm will be limited to network personnel, the Operations Manager, and senior IT managers at the AVP level and above.
>
> Access cards will only be issued to individuals with a legitimate business need.

Individuals issued an access card will NOT loan their access cards to other individuals.

If an access card is lost or stolen, it is to be reported as soon as practical to Deerwood Security and the Director, Technology Administration. Subsequently, the card's access will be terminated.

When an individual leaves employment at the College, their access card will be returned to the Director, Technology.

The AVP of Technology Operations and the CIO may request a summary report of access to the NOC for review.

The AVP of Technology Operations and the CIO will perform a periodic review of names and access levels.

All visiting personnel must be accompanied by at least one member of IT and will be required to check-in and checkout at the front desk where they will fill out the logbook and be issued a visitors badge.

09-02.13 • ERP SYSTEMS SECURITY [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to describe Enterprise Resource Planning systems security relating to the host operating system.

Description/Procedure:

The main component of Florida State College's Enterprise Resource Planning (ERP) system, ORION is housed on an Oracle Enterprise Server running Solaris Unix operating system (OS). Security for access through the OS is controlled by and the responsibility of the Open Systems Team. Specifically, access is accomplished using a Keyboard Interactive prompt that requires a log-on ID and password. Users utilize Hummingbird Terminal emulation software, which communicates with the server via SSH. The user is prompted for their UNIX username & password. Upon successful UNIX authentication the user is presented the Natural ORION Menu screen. The user's Natural account is verified using OS authentication. Issuance and retraction of log-on ID's and passwords is the responsibility of the Open Systems Team upon request by Human Resources. The Open Systems Team and DBA, in conjunction with the Human Resources department, will monitor UNIX access to validate legitimate business needs for such access.

09-03.13 • ERP APPLICATIONS SECURITY [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to describe the Enterprise Resource Planning (ERP) applications security for the ORION system.

Description/Procedure:

Security for the ERP applications portion is provided within ORION from two levels. First there is security native within Software AG's Natural programming environment (Enterprise System-level Access). The database administrators manage security access to the enterprise application environment, granting database access with the creation of an enterprise system-level access account. Additionally, when notified by Human Resources, they are responsible for suspending or terminating access when an individual leaves employment of the College or no longer has a business need for access. This termination of accounts also includes any accounts that have not been accessed within six months or any new account not accessed within the first 30 days after creation.

Enterprise System-level Access only allows the user to navigate to the appropriate menu screens for the various application modules within ORION – it does not provide access to modules. The second level of applications security is native within ORION itself and does allow access to the function modules e.g. purchasing, A/P, registration, etc. The user group managers from each functional area controls access from this level. Essentially, access to the ORION applications / modules is a two-step approach:

Enterprise System-level Access

Access to the ORION Applications (modules)

The designated system owners (user group managers) are responsible for the development and management of processes dealing with the provisioning of user security/module access (APM 07-0303). A batchjob (SEC007J1) within the ORION batch submission menu is available for the primary users to monitor global access to their systems.

09-04.13 • DATA SECURITY [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to describe the security requirements for internal and external college systems.

Description/Procedure:

Information Classification

Information must be classified to ensure appropriate security controls are applied.

- Public Information - Public information poses no risk to the college if it should become public, or it may already be in the public domain
- Sensitive Information - Sensitive information is intended for distribution within the college on a highly limited and restricted "Need-to-Know" basis only. This included personally identifiable data.

Encryption

Data encryption should be used to protect the confidentiality of critical or sensitive information sources.

- All sensitive data should be encrypted.
- Sensitive data must be encrypted when transmitted outside of physically secured areas.
- Sensitive data must be encrypted when data resides in physically unsecured areas.
- Sensitive data should be encrypted when not actively in use.
- Sensitive data should be encrypted when stored on hard disks.
- Data should be encrypted when transported in computer-readable storage media, such as magnetic tape, floppy disk, CD-ROM, or any other removable media.
- Original documents should be deleted only after the user has demonstrated the ability to recover the original document from the encrypted data.

Encryption Algorithms

The following are encryption approaches used by E-Systems for encryption of data:

- Pretty Good Privacy (PGP) (Supported Versions)
- Advanced Encryption Standard (AES)

Data Labeling

All information assets or information processes, from the time of creation until they are destroyed, should be labeled (marked) using the classification scheme for confidentiality.

Application of classification labels

No specific security labeling controls are required for labeling public information.

- For sensitive data, the label must identify the owner.
- Label indicates the highest classification of data contained.
- Labels are to be applied uniformly, leaving no doubt about the classified status and the level of protection required.
- For documents, label must appear on the cover page and at the top of each interior page, indicating the level of classification and owner.
- For very sensitive information, specifically indicate individuals for distribution.

Unlabeled Information Resources

- When an information asset does not contain a classification label, it is assumed to contain sensitive information.
- Output from information systems containing classified information carry the appropriate classification label
- If the information clearly contains student or financial information, the information resource must be treated as “Sensitive ”

Reclassification of Information Resources

Responsibility for changing the classification of an information resource lies with the Application Owner.

09-05.13 • ROOT/SYS ADMIN ACCESS [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The intent of this section is to outline the policies and procedures associated with Root/Administrator access on the various server, network and computer systems used at the college.

Description/Procedure:

It is the policy of the Information Technology department to grant individuals the least privileged access to a system as is required for them to accomplish their job function or task.

Root access on college wide UNIX servers and Enterprise Administrator access on the Florida State College Active Directory forest and to all network and telecommunications equipment is limited to the appropriate members of IT, under the direction of the Associate Vice President of IT for the associated system.

The Associate Vice President of IT may grant sufficient rights to campus technical support personnel to campus-based servers or network equipment at their locations on the basis of need. These rights may or may not be granted based on the demonstrated skills and the level of trust of the individual. End Users and groups are not allowed or provided the ability to grant Root or Administrator privileges to others. The Florida State College Enterprise Administrators group is to have Administrator privileges on all member servers in the Florida State College Active Directory forest and all other servers and workstations on the production network. All Servers and desktop computers must be placed in the Domains and Workgroups approved by the Associate Vice President of IT – Technology Operations. While Faculty and Staff are to be granted Local Administrator Level Access for their assigned laptops, Administrator access must still be granted by the Enterprise Administrators.

Any requests for elevated network access levels must be submitted through the Helpdesk/Learner Support Center to the IT Department for consideration.

09-06.13 • ERP DISASTER RECOVERY [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

Florida State College at Jacksonville (Florida State College) is heavily dependent on automated systems and IT for daily operations. As such, the purpose of this section is to delineate the College's Information Technology (IT) Disaster Recovery Plan. The section will provide the procedures utilized by IT in order to have Florida State College's daily operations completely functional within 72 hours should Florida State College at Jacksonville experience a catastrophic event.

Description/Procedure:

There are four (4) distinct segments to the Information Technology Disaster Recovery Plan. These segments are:

Scheduled full and incremental file/system back-up procedures that ensure Florida State College's ability to restore systems, in the event of system problems or disaster.

Procedures for continued processing of the Florida State College's staff faculty payroll, locally or remotely.

Procedures for restoring the physical computing infrastructure/hardware leading to restoration of enterprise operations from back-ups in the event of a disaster.

Development of a College Command Center to serve as an operation center during a disaster.

IT Disaster Recovery and Business Continuity Plans are currently have been developed with LBL Technology Partners. This plan outlines necessary procedures to ensure business continuity with minimal down time in the event of a disaster.

09-07.13 • BACK-UP RESTORE PROCEDURES [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The intent of this section is to describe backup and restore policies and procedures of network servers and equipment by the IT Department.

Description/Procedure:

The Engineer V - UNIX Systems Team is responsible for all backups and the reporting and all coordination of all backups. Network Operations Center (NOC) based servers and the Information Technology department for the purpose of recovery in the event of a hardware or software failure backs up network equipment configurations regularly. Full backups of college wide email, web, application and file servers are scheduled weekly. Incremental backups are scheduled nightly on days that full backups are not scheduled.

All campus-based servers are backed up by the Information Technology department. For information on backup of campus-based servers, contact your individual campus-based technical support department.

Sometimes corrupt or accidentally deleted files can be recovered, but the best solution for students, faculty and staff is to always keep backups of important data. In the case of a server failure or other loss of data, the Information Technology staff will restore the data and work to assist campus-based personnel as needed in the recovery process.

End-user responsibilities:

- The Information Technology department does not back up files stored on workstations; backups of user data and information are the responsibility of the end user.
- Instructors are expected to keep backup copies of their web pages, course work, email and other important data.
- Students are expected to keep backup copies of their work. This includes web pages published on the College's web servers and class work.

09-08.13 • EVACUATION PLAN [ADEEB]

Recommended By: Patty Adeeb, Executive Director, Deerwood Center

Purpose:

The purpose of this procedure is to identify an evacuation plan for the Deerwood Center in case of an emergency.

Description/Procedure:

In case of fire or emergency:

- Sound alarm by voice or fire alarm box
- Notify Security or Maintenance; provide your name and area of the fire or emergency
- Notify Executive Director or Site Maintenance Manager if security/maintenance not reached
- Security will notify all other appropriate parties and direct the process
- Emergency marshals, if safe and possible, shall go immediately to his/her designed location to warn others and direct them from the building
- Site maintenance supervisor will report to the emergency area to locate fire or emergency
- If false alarm, maintenance will alert security, and security will cancel call and reset system to normal

Evacuation:

- During evacuation, remain calm, and proceed safely, orderly, and expediently
- Elevator use is restricted for the handicapped and injured only

Security will:

- Authorize evacuation process
- Announce, along with emergency marshals, to evacuate
- Insure all areas are evacuated, along with emergency marshals
- Emergency marshals will:
- Insure his/her designated area is evacuated
- Inspect elevators for any personnel or students, and

- If possible, secure property for college

Faculty will:

- Direct his/her students to nearest exit out of building
- Have students assist handicapped students in the evacuation
- Remove, if possible, all personal book bags and valuables
- Students, staff, and tenants will:
- Follow directions of faculty, security, or emergency marshals
- Proceed to nearest exit out of building
- Assist handicapped students in the evacuation
- Remove, if possible, all personal items and valuables
- All personnel, except security, are to proceed to the nearest parking lot (100 feet from the building), taking care to move as far as possible from the entrances to prevent interference with the arrival of emergency personnel and equipment
- All shall remain outside the building until notified the emergency is over and instructed to return to original locations
- Security will monitor the control system, maintain order, and direct emergency personnel; plant operators will eliminate the supply for gas, electrical, and mechanical functions

In case of a hurricane or other weather disaster:

All faculty, students, and staff will evacuate the building in an orderly, safe, calm, and expedient manner not later than twelve daylight hours before the estimated time that winds will reach 45 m.p.h.

Security will:

- Issue hand held radios and batteries to safety team members and director
- Monitor and restock emergency supplies
- Monitor all communications and warning systems
- Develop a duty roster to provide at least one officer per campus during the passing of the storm

- Establish coordination with appropriate law enforcement agencies and obtain any special instructions required for after-storm security backup

Plant service staff will:

- Ensure all roofs and outdoor areas are clean of unsecured equipment
- Ensure down spouts are clear
- Top off fuel tanks on all vehicles and generators
- Relocate outdoor equipment and temporary structures to storages areas (signs, small vehicles)
- Install plywood over glass windows and doors if not covered with a glass protection product called armor-coat
- Clear shelves and desks of loose objects and store bagged items
- Cover furniture with plastic bags and securely taped
- Move furniture away from windows
- Unplug cords and close all doors

Business office staff will:

- Arrange for and stand by to deposit all on-hand funds to the bank, except for a minimal operational budget not to exceed $50.00
- Backup all computer data and prepare to relocate essential diskettes, tapes, files and media
- Clear shelves and desks of loose objects and store bagged items
- Cover furniture with plastic bags and securely taped
- Move furniture away from windows
- Unplug cords and close all doors
- Faculty and staff will
- Backup all computer data and prepare to relocate essential diskettes, tapes, files, and media
- Clear shelves and desks of loose objects and store bagged items
- Cover furniture with plastic bags and securely taped
- Move furniture away from windows

- Unplug cords and close all doors
- President or Executive Director, Deans, and Associate Deans shall identify temporary storage for critical documents, equipment (no interior windows); security shall provide special pressure sensitive evacuation labels; eight hours required to prepare the building.

Preventive Safety Measures:

- All faculty, staff, and students should exit the building in pairs or seek security escort if leaving after dusk.
- All faculty and staff should lock valuables in a desk or cabinet upon leaving their office for an extended period of time.
- All faculty and staff should lock their office doors upon leaving their work area.
- If you see someone in the center that appears suspicious, please alert security.
- All faculty and staff should report the loss of office keys and swipe cards immediately to security.
- All faculty should remind students to report suspicious persons to security and walk in pairs or with a security escort to their cars after dusk.
- All faculty, students, and staff are required to have an Florida State College photo ID for identification and access to areas during recovery operations.

Emergency Marshals	Alternates	Assigned Areas
Zoran Bozic (x2749)	Katie Haft (x2790)	Bottom Floor - Academy
Michael Rupright (x2750)	Lisa Reinertson (x2749)	Bottom Floor - NOC Side
Ed Robinson (x2588)	Frank Heinz (x2502)	Top Floor - NOC Side
Robin Sarge (x2708)	Wende Frey (x2506)	Top Floor - Academy
Amanda Le (x2716)	Trina McCowan (x2562)	Top Floor - G-Wing
Norine Katich (x2611)	Robert Oberholtzer (x2749)	Bottom Floor - G-Wing

Table 9.1: Emergency Marshals

Security Officers	Executive Director	Assistant to Executive Director	Site Maintenance Manager
Sgt. Sharrie Hines (x2650)	Dr. Patty Adeeb (x2564)	Lorna Pryor (x2717)	Zoran Bozic (x2749)
Officer David Wilhight			
Officer Deborah West			
Officer Joy Ellis			
Officer Joshua Gardner			
Officer Marvin Dorisca			
Officer Samuel Anderson			
Officer Joshua Simmons			

Table 9.2: Security Officers

Safety and Security Telephone Numbers	
Emergency Telephone Numbers:	
Jacksonville Sheriff's Office	911 or 630-0500
Jacksonville Fire Department	911 or 630-0529
Jacksonville Rescue Department	911 or 630-0529
Jacksonville Electric Authority	632-0300
Jacksonville Civil Defense	630-2472

Table 9.3: Safety and Security Telephone Numbers

Safety/Security Department	
Deerwood Security (Sgt. Sharrie Hines)	(O) 997-2651; (C) 487-3756
Officer David Wilhight	(O) 997-2650; (C) 466-7864
Zoran Bozic	(O) 997-2749; (C) 899-2318
Patty Adeeb, Exec Dir.	(O) 997-2564; (C) 316-7970
Stan Jurewicz (Dir. Risk Management)	(O) 632-5054; (C) 505-8627
Mike Pindell (Fire Marshall)	(O) 632-3110; (C) 626-4195

Table 9.4: Safety/Security Department

Security Problems	
Deerwood Security	997-2650 or 997-2651
Sgt. Sharrie Hines	(C) 487-3756

Table 9.5: Safety/Security Department

Facilities Maintenance (After Hours)	
A/C (Zoran Bozic)	(C) 899-2318
General Elevator	1-407-859-4340

Table 9.6: Safety/Security Department

Hazardous Materials Notification List:	
Jacksonville Sheriff's Office	911 or 630-0500
Jacksonville Fire Department	911 or 630-0529
Jacksonville Rescue Department	911 or 630-0529
Department of Environmental Regulations (JAX)	448-4320; x359
Department of Environmental Regulations (TAL)	7-1-488-1320
National Response Center	1-800-424-8802
Environmental Protection Agency (Atlanta)	1-800-347-4062
Florida Highway Patrol	359-6680
Hazardous Materials Coordinator – Feliche Muccioli	632-3112; (H) 924-1453; (C) 813-1804
Fire Safety Inspector – Mike Pindell	(O) 632-3110; (C) 626-4195
Poison Control Center	387-7500 or 1-800-282-3171

Table 9.7: Hazardous Materials Notification List

09-09.13 • ENVIRONMENT ALARMS [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The intent of this section is to describe the Information Technology Department's environmental alarm system for the Data and Network Operations Center.

Description/Procedure:

The College utilizes dedicated hardware and software systems to monitor environmental conditions in the Data and Network Operations Center computer rooms. The systems monitor and provide automatic alerts via audible alarms, text paging and email to appropriate personnel for the following events:

- **Temperature** (i.e. HVAC problems)
- **Humidity** (i.e. HVAC problems)
- **Main Power** (i.e. power failure)
- **UPS Power** (i.e. power failure)
- **Flooding** (i.e. HVAC chilled water leaks, etc.)
- **Smoke** (i.e. electronic component burning, fire)
- **Panic** (i.e. user presses the 'panic button' for help)

09-10.13 • NIPC/INFRAGARD [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this policy is to ensure that all technological applications and processes of Florida State College at Jacksonville are operating within federal security compliance standards set forth by the National Infrastructure Protection Center (NIPC) and the FBI INFRAGARD program.

Description/Procedure:

The College will, within its power, maintain technology operations that are fully compliant with the policies of the NIPC and INFRAGARD.

The College will maintain active membership in the Local INFRAGARD Chapter.

The College will fully cooperate with all local, state, and federal law enforcement agencies in regards to information and technology security.

09-11.13 • FIREWALL ADMINISTRATION [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this Policy and Procedure is to outline the firewall administration procedures for Florida State College's production network.

Description/Procedure:

Florida State College at Jacksonville utilizes redundant Cisco ASA and PIX Firewalls, operation in failover mode.

Firewall configuration rules and permissible service rules have been reached after an extensive evaluation of costs and benefits to the organization. These rules must not be changed unless the permission of the Associate Vice President of IT – Technology Operations, or the assigned firewall administrator, has been obtained.

Change requests must include the IP addresses of the destination systems, as well as the source systems that will require access. (Source Systems may include "all public addresses" if needed.) The request will also need to contain a list of the minimum necessary ports that will need to be opened, a description of the service, as well as the benefits to the College as a whole. These factors will be weighed against the risks and may or may not be approved.

Unless authorized by the Associate Vice President of IT – Technology Operations, all systems made available to the public through the firewall must be located at the Network Operations Center and be Administered by the Technology Department. Static IP Addresses will need to be assigned and if the addresses are internal, Network Address Translations to public addresses will need to be assigned.

09-12.13 • WIRING STANDARD [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of the procedure is to provide standards for all telecommunications and network wiring projects college wide.

Description/Procedure:

The Associate Vice President of IT – Technology Operations defines the wiring specifications for all telecommunications and network wiring project throughout the college. These standards are available to the Facilities department, the Campus DASes and Contractors. The Current Standards can be found on the Technology Division's website, Technology Plan page as Information Transport System Specifications.

10-01.13 • PMBOK [REIMAN]

Recommended By: Dennis Reiman, AVP, Tech, Associate CIO & CTO

Purpose:

The purpose of this section is to define the reference for project management standards used for the planning of technology projects.

Description/Procedure:

The Project Management Body of Knowledge (PMBOK) by the Project Management Institute (PMI – http://www.pmi.org) establishes the guidelines used for the planning of technology projects.

10-02.13 • METHODOLOGY .NET/JAVA ARCHITECTURE [REIMAN]

Recommended By: Dennis Reiman, AVP, Tech, Associate CIO & CTO

Purpose:

To identify the programming methodology used to architect systems built with the .NET framework and Java Technology.

Description/Procedure:

The E-Systems group will use eXtreme Programming (XP) as the development methodology. This methodology stresses customer satisfaction while allowing the developer to quickly adjust to the changing needs of our customers.

The E-Systems Team will:

- Constantly communicate with fellow programmers and customers
- Keep the design simple
- Get constant feedback through testing
- Deliver the product as early as possible
- Respond to change requests from the customer

The E-Systems group embraces web services technology in the design of integrated systems. System design permits the sharing of data driven functions with systems external to the E-Systems environment. (Examples: Blackboard, other institutions, etc.) Services/Transactions are driven through web services as part of the web application portfolio.

10-03.13 • ADABAS REFERENCES, ETC. [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to identify ADABAS Reference Resources. This procedure enables the Database Administrators (DBAs) and application programmers to reference additional resources for performing database operations.

Description/Procedure:

- Utilities
- Command Reference
- Messages and Codes
- Administration
- Extended Operation

Additional resources from Software AG:

- Release Notes
- Installation
- Adabas SQL Gateway manuals
- Natural/Natural Security/Predict Manuals
- (See link below for Software AG Website)

Internet Sites:

http://www.softwareag.com/adabas/

https://empower.softwareag.com/products/documentation/default.asp

http://www.gensystems.com/booklist_ADABAS.htm

10-04.13 • NATURAL PROGRAMMING GUIDES [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to identify Natural Programming Resources. This procedure enables the application programmers to reference additional programming resources.

Description/Procedure:

- Natural Developers Handbook
- Natural Construct Application Development User's Guide
- Natural Construct Tips & Techniques
- Developing Natural Systems
- Natural Study Guide
- Advanced Natural Study Guide

Additional resources from Software AG:

- Natural Construct Fundamentals
- Natural Programming Foundations
- Predict Fundamentals
- Natural Tips and Techniques

Internet Sites:

- http://www.softwareagusa.com/education/pubonlinecat.asp?PARENT=&MENUITEM=services8
- http://www.gensystems.com/booklist_Natural.htm
- http://www.gensystems.com/booklist_NaturalConstruct.htm
- http://communities.softwareag.com/codesamples
- http://communities.softwareag.com/wiki/

10-05.13 • EXTREME PROGRAMMING [REIMAN]

Recommended By: Dennis Reiman, AVP, Tech, Associate CIO & CTO

Purpose:

The purpose of this section is to describe the disciplined approach to software development used by E-Systems Technology.

Description/Procedure:

E-Systems Technology develops and supports advanced web applications that enhance the student's experience at Florida State College. The dynamics of E-Systems projects require a disciplined approach for rapid but high quality development. The eXtreme Programming methodology (XP) provides the environment for developing highly available products that quickly meets customer's needs and satisfactions.

Four (4) primary categories of rules and practices exist for the XP methodology:

Planning:

- "User Stories" – Written by customers describing what they need the system to do.
- "Release Planning" – Development of project plan (refer to 06-04 – Development)
- Development and Implementation of small releases (development not released as "versions"
- "Move people around" – Developers are rotated/cross trained through the different systems/ subsystems.

Designing:

- "Simplicity" – Applications are initially developed and released with a simple design (faster and cheaper). Provides access to customers quicker than developing a complex system. Enhancements can be identified and are made with same process using the XP methodology.
- "Never Add Functionality Early" – Keep the application uncluttered by not including additional functionality unless the clients specifically request it.

Coding:

- Customer Availability – Coders must communicate with the customer to ensure the "user story" is met by the system functionality as it is developed.
- Coding Standards – Development must follow identified coding standards (refer to 06-08 - E-Systems – Programming Standards)
- No Overtime – Projects are reviewed with customer to review/change the project scope, identify additional resources, and to review/change the timeline (as appropriate) if the project is behind schedule.
- Optimize Last – "Make it work, make it right, then make it fast."

Testing:

- Code Review – Application/enhancements are tested and reviewed by all E-Systems Team members.
- Unit Tests – When bugs are found, it is documented and tested each time to prevent it from reoccurring.
- Customer Approval – Customer ensures "user story" is met by functionality and agrees for its release.
- Release – The Director, E-Systems must approve before it can be released.

Additional information on the eXtreme Programming can be accessed at http://www.extremeprogramming.org/.

10-06.13 • SCRUM [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this Technology Policy and Procedure is to describe the use of the SCRUM project management method to manage and control the development of large multimedia software development projects.

Description/Procedure:

The Multimedia Technology Area develops large multimedia software applications for use as computer-based training (CBT) or computer aided instruction (CAI). Due to the large size and long development cycles inherent in these projects it was necessary to adopt the SCRUM method of project management.

The SCRUM method has 3 primary categories of implementation

- Planning

Customer meeting and commitment

Storyboard, flowcharts depending on nature of project

Small milestones are set

Timelines are set

Customer agrees to plan and signs off on it

- Production

All aspects of production move forward simultaneously

Customer is involved during every step providing QA

Small milestones are achieved at a rapid pace.

Small 15 minute one on one informal meeting are held to ensure daily progress

Full team meetings (1 hour) are held every week to ensure everyone is working together

- Delivery

Since the customer has been providing QA throughout the project; this is a short step

Customer signs off on receipt of product

The SCRUM method is very simple non-linear approach to large project management. The main aspect of SCRUM that sets it apart from the rest is located in the production phase. As stated above all aspects of production move forward simultaneously. Traditionally production moved forward in a linear fashion, hence the term “production line”. In those terms, SCRUM can more accurately be termed as a “production wave.” Everyone is side by side working on the same task towards the same small milestone. Many milestones put together have the potential to create large projects in a quick and efficient manner.

Additional information about SCRUM can be found at http://www.controlchaos.com

11-01.13 • INTERRUPTION OF PHONE SERVICES (SYSTEM FAILURE) [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this section is to describe the general process for handling interruption of phone service Collegewide.

Description/Procedure:

Florida State College has contractual agreements with various vendors for providing telephone service..

When telephone service is interrupted at any campus/center, it is to be reported to the HelpDesk. Once notified, the Telecom group will determine the probable cause and involve the appropriate vendors to effect resolution. Generally, outages will be reported Collegewide via email, with appropriate updates and final resolution.

12-01.13 • DEFINITION [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to describe the functions and technical environment of the Data Management Team.

Description/Procedure:

Data Management includes the following functions: Data Base Administration for Enterprise Databases and Disaster Recovery Coordinator for the Enterprise Applications team.

12-02.13 • STRUCTURE [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to describe the functions and responsibilities of the teams within Data Management.

Description/Procedure:

Database Administration

Database Administration is responsible for the design, specification, development, and integrity of all databases used by Information Systems at Florida State College. The team manages the database environment for Florida State College's information technology department

Specific responsibilities include, but are not limited to:

- Database design
- Database Administration
- Data Warehouse Design and Implementation
- Database Backup and Recovery
- Data Integrity
- Data Management Standards
- System Tuning
- Reporting of Utilization and Performance

Enterprise Applications Disaster Recovery Coordinator

Specific responsibilities include, but are not limited to:

- Coordinate the development and testing of disaster recovery and business continuity procedures for the Enterprise Applications team.
- Schedule Disaster Recovery tests for the Enterprise Applications team.
- Ensure the accuracy of the Enterprise Applications Disaster Recovery documentation

12-03.13 • DEVELOPMENT [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to describe the development processes of Data Management.

Description/Procedure:

Requests for new Data Management development projects (new databases, changes to existing databases, and cube processing applications and enhancements) must be submitted to the Data Management team via the IT Request System. A reply will be sent within three (3) business days to the requesting party.

The Data Management team prior to procurement/installation must approve Enterprise Database products.

Project acceptance and prioritization are established by the Executive Director, Enterprise Applications based on an analysis of project need (net-benefit), size, scope, and cost. User groups can establish the priorities within the IT Request System.

The approved project management instrument (refer to 05-02 – Project Management Standards) will be used.

Project (application) development must occur in a test environment to ensure that the production system is not affected by the development (refer to 06-05 – Testing).

12-04.13 • TESTING [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to describe the testing methodology used by Data Management.

Description/Procedure:

For Software AG and related products the following procedures shall be used:

Upgrades to software relating to the ORION environment will be implemented with the following steps:

- It will be implemented in the systems testing area that is separate from all other users.
- It will then be implemented in the test environment and the applications staff will be able to test it. The Application Systems and E-Systems staff will be notified via e-mail when the installation will take place and again when it has been implemented.
- It will then be implemented in the acceptance environment, which will give the user group the ability to test it out. The Application Systems, E-Systems, and User group areas will be notified via e-mail when the installation will take place and again when it has been implemented.
- It will then be implemented in the production environment. The Application Systems, E-Systems, and User group will determine the implementation date based on the college calendar. An e-mail will be sent college wide regarding the installation, an e-mail will be sent to the help desk notifying them of any downtime and the E-Systems team will put a notice on Artemis.
- A back out plan will be in place if needed.

Note: The installation will go to the next step when the group that is testing it is satisfied that everything is working fine. Each implementation step will include e-mail communication with the appropriate groups.

Other Database Software Infrastructure Testing

When the development environment is upgraded with a new version or service pack, the DBA group will schedule the upgrade for minimal interference with ongoing projects.

Prior to installing the upgrade in production, a list of checks will be made to ensure that no production systems are adversely impacted by the upgrade.

A means to roll back the upgrade will be planned in case any problems are found in the testing phase.

The DBA group may require the assistance of other groups in assembling a list of QA checks to make following a particular upgrade.

SQL Server-based application and database testing

Whenever the DBA group creates new stored procedures, DTS packages, or other elements to be eventually used in production systems, they will subject those elements to testing in the development environment to ensure that they produce the expected results before deploying.

Whenever the E-Systems group creates new stored procedures, or other elements to be eventually used in production systems, after testing to ensure that they produce the expected results, will submit a request to the Data management team to review and/or test to ensure that the expected results are produced in an efficient manner before deploying and that the proper programming guidelines have been adhered to.

If testing is needed in the production environment it will be isolated from existing productions systems and made available to only those testing.

12-05.13 • PRODUCTION [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to describe the procedures for the testing and migration of applications developed by Data Management into the production environment.

Description/Procedure:

New applications/releases/upgrades must be developed and tested in a test environment (refer to 06-05 – Testing). If applicable, user group managers/directors must provide written authorization prior to release into a production environment.

Hot fixes (emergency corrections) to the system are to be migrated into production at the discretion of the Director Information Systems (Applications). If down time is required for the migration of the hot fix, the appropriate (and applicable) groups/individuals will be notified regarding the problem from the contact list (see example below).

The migration of data to the production environment must also be planned and coordinated with the release of corresponding applications.

The Director of Information Systems (Applications) is responsible for assigning the team member responsible for the migration of programs and data into the production environment. Following the migration of new applications or enhancements, the system must be thoroughly tested to ensure system integrity and validity.

Contact List

- Database Administrator
- Director, Applications
- Director, E-Systems
- E-Systems Team members
- Technical Help Desk
- User groups (managers)

12-06.13 • DBMS STANDARDS (ADMIN) [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to describe the procedures for the development and maintenance of databases supported by Data Management.

Description/Procedure:

The Data Management Team ensures good design of, develops, manages, and supports database applications for the following environments: Microsoft SQL Server, Software AG Adabas, and Oracle.

Database Design Guidelines (SQL Server)

1. Every table must have a primary key field.
2. Avoid using composite primary keys. Use one primary key field, with unique indexes placed on the other columns to make the data row unique.
3. Column names are normally to be singular attributes (not pluralized).
4. Column and table names should be in the following notation: ThisTableName ThisColumnName. No underscores, spaces, dashes, or other non-alphanumeric characters.
5. Tables, columns, and other objects should not be named using reserved words.
6. Avoid storing calculated data in OLTP databases.
7. Either use full name or comprehensible abbreviation.
8. A composite table, that is, a table designed primarily to create a many-to-many relationship between two or more other tables, should be named by concatenating the names of the tables it joins. For instance, a table joining Farmers and LivestockTypes should be called FarmersLivestockTypes

Database Design Guidelines (All databases)

1. Tables, columns, and other objects should not be named using reserved words.

2. DBAs shall be responsible for planning and implementing indexes on database tables. They will work with programmers, users, and management when questions arise about usage that would influence indexing decisions.

Database Programming Guidelines

1. In most cases, data modifications should be handled through stored procedures, Data Transformation Services (DTS) packages, and/or User-Defined Functions.
2. Stored Procedures will be reviewed and/or tested by the Database Administrators. The DBA should be notified as soon as the code is available in the development environment.
3. If JOIN statements are used, they must be in the FROM clause (unless otherwise approved by the DBA).
4. Columns used in the FROM clause as joins or in WHERE clause must be checked for indexes.

Database Schema and/or Database object changes

1. Any database schema change to a production database should be performed by a DBA.
2. All database migrations should be done by a DBA.
3. All changes to database structure should be requested by means of an e-mail to the SQL Server DBA group so that DBAs can make recommendations on database design before code is written based on that design. If the change is not done immediately, a DBA will respond promptly with a time frame for completion. The DBA will also confirm when the change is done.
4. If the change(s) cannot be made within the required timeline, the developer may make the change(s) and forward to the DBA for approval.

Database Backup and Recovery

1. Database backup files must be placed on a separate physical drive (or secure storage medium).
2. Programmers should request any necessary backups for SQL Server development databases.
3. A quarterly review of the backup jobs will take place.

4. DBAs should be informed if a database will not be or is not used.

Performance Monitoring

Archiving

1. DBAs will not initiate or specify what data should be archived with what parameters but will set up archive processes as requested.

Comments

Commenting can be a valuable and time saving technique when done properly.

- Comments should be written explaining ‘why’ instead of ‘how’.
- Comments should make statements about the code that the code itself cannot.
- Comments should not emulate the code.
- Header comment will contain, at a minimum:
    - Author
    - Original Date
    - Purpose
    - Modification History
    - Name of migratory and date of migration to production
- Comments that are added by a programmer other than the one listed in the header comment section should contain the user ID and date.
- Example: “This block of code was modified mm/dd/yy. <Userid>

Security

No sensitive data should be stored on personal devices.

We will not download or give access to data without prior written consent from the owner of the data and a full understanding/education process for all involved.

12-07.13 • CONFIDENTIAL COLLEGE INFORMATION ON CONSULTANT/ VENDOR EQUIPMENT [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to describe the procedures for handling confidential College information on Consultant or Vendor equipment.

Description/Procedure:

No sensitive data (personally identifiable data or confidential information) should be stored on personal devices, whether they are physically working at the College, or if they are working remotely.

Contractors are required to sign a confidentiality agreement upon commencement of their contractual services.

13-01.13 • TECHNOLOGY SUPPORT SERVICES [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to present procedures relating to the resolution of problems encountered in the operation of College technology resources.

Description/Procedure:

The following outlines the process for receiving College related Technical Support Services is as follows:

1. For Learning Management System (LMS) Support, dial 904-632-3151 or 866-886-4952 then choose Option 1. This call will be routed to LMS Support. They will attempt to resolve the issue by phone, otherwise it will be routed to the College LMS administrator.
2. For issues logging in to the Employee Portal or Connections, dial 904-632-3151 or 866-886-4952 then choose Option 4. The technical call center will attempt to resolve the issue by phone, otherwise it will be routed to the College systems development support team.
3. If you have an issue that deals with technology on a campus (workstations, smart classrooms, etc.), call 904-632-3151 or 866-886-4952 then choose Option 3 for Campus Support. (Or see Campus Support contact information below.)
4. For all other technical issues, you should dial 904-632-3151 or 866-886-4952 then choose Option 4. The technical call center will make all attempts to assist, and will forward the ticket to the appropriate College resources as necessary.

The Helpdesk Website & Knowledge Base is located at: http://help.fscj.edu

If you need Campus Support, please contact them directly either by e-mail or phone. The most current contact information can be found at http://www.fccj.org/friends/foremployees/empcomputing/index.html

You can also find support for Blackboard and software applications at the Faculty Resource Centers located at a campus/center. http://www.fscj.edu/techteam/learning-innovations/section/faculty-resources

For Blackboard Training Classes:

Go to Artemis and select the College tab for the AFPD Catalog (Academy for Professional Development). http://www.fscj.edu/techteam/learning-innovations

13-02.13 • VOICEMAIL [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this section is to describe the basic guidelines for usage of the College's voice mail system.

Description/Procedure:

Florida State College utilizes a Cisco IP Telephones and a Cisco Unity Voice Mail System. Employees should access their messages routinely and clear their mailboxes. The administrators of both systems reserve the right to delete all old voice messages when space is limited, to avoid saturation of the system, which can lead to an inability to leave voice mail messages College-wide.

13-03.13 • MOVES, ADDS, AND CHANGES (MAC) [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this section is to describe the process for Moves, Adds, and Changes (MAC) for telephone service Collegewide.

Description/Procedure:

The college utilizes a Cisco IP Phone System and is maintained by Florida State College's Network Infrastructure and Telecommunications Team.

Requests by an end user that requires service to be moved, added, or changed, should be sent to the their campus Director of Administrative Services (DAS) through either email or a telephone call. The DAS will initiate a corresponding MAC request to the appropriate system administrators.

13-04.13 • SERVICE REQUEST PROCESS [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to describe the procedures associated with generating the task list for each application area.

Description/Procedure:

The Technology Team has implemented an IT Request System (JIRA) whereby a task list is maintained for the Application Development area. Each task list is a representation of the full workflow of tasks pertaining to a particular application area. If an end-user has the need to have an item placed on a task list, the end-user should submit an issue through the IT Request System to the Applications Development project via the Employee Portal. The issue should specify the components, environment brief description, type of issue, reason for issue, priority of issue and the time frame for which the issue is desired to be completed. Additionally, screen shots and wireframes can be attached to the request. At the discretion of the Directors of Information Systems (Applications and E-Systems), issues may be forwarded to the Executive Committee for prioritization.

All issues can be tracked and followed within the IT Request System (JIRA).

13-05.13 • ERP SYSTEM AVAILABILITY SCHEDULE [MARTIN]

Recommended By: Chris Martin, Executive Director, Enterprise Applications

Purpose:

The purpose of this section is to outline availability for the College's Enterprise Resource Planning (ERP) system, ORION.

Description/Procedure:

ORION will be available for registration, online functions, and online batch processing as denoted below:

Day	Time
Sunday	7:00 a.m. - 9:00 p.m.
Monday	7:00 a.m. - 9:00 p.m.
Tuesday	7:00 a.m. - 9:00 p.m.
Wednesday	7:00 a.m. - 9:00 p.m.
Thursday	7:00 a.m. - 9:00 p.m.
Friday	7:00 a.m. - 9:00 p.m.
Saturday	7:00 a.m. - 9:00 p.m.

Table 13.1: Batch Processing

These times represent the minimum amount of time ORION will be available. The second Sunday of each month is reserved for regular maintenance and upgrades and will supersede the scheduled availability noted above. The last day of each month is reserved for month-end runs, and the last two weeks of the fiscal year are reserved for year-end runs and will take precedence over the normal availability schedule. System outages required for maintenance, port upgrades, product upgrades, etc. are discussed with the user community prior to altering the normal availability scheduling.

The scheduled maintenance downtime for servers within the Technology Department and Collegewide is located on the College Technology Department website http://www.techteam.fscj.edu/maintenance_downtime/index.php. This 5-year schedule is planned in advance and approved by the Florida State College Cabinet Members.

13-06.13 • NETWORK LOGIN [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The intent of this Technology Policy and Procedure is to identify information relating to network logins. Full-time faculty, adjunct faculty, staff (full and part time) and approved contractors can be granted a computing account to access to Florida State College network resources with the appropriate documentation.

Description/Procedure:

Access to college computing facilities is a privilege granted to students, faculty and staff. Access to the college's computing resources is granted solely for the pursuit of scholarly activity and/or other activities related directly to the mission of the college. Access is granted subject to adherence to generally accepted ethics. Unapproved or unethical use of computer access may be grounds for revocation of this access. Users and system administrators must all guard against abuses that disrupt or threaten the viability of all systems, including those at the college and those on networks to which the college's systems are connected.

All users are subject to the College's Acceptable Use Policy (Acceptable User Policy - Students, Acceptable User Policy – Faculty and Staff and as published in the College catalog), all Administrative Procedures and Policies (as published in the College's Administrative and Procedures Manual), all Rules of the District Board of Trustees and all applicable state and federals laws governing the use of computers, networks, and associated resources.

Faculty and Staff

An employee computing account is required to gain centralized, authenticated access to basic network resources including, network printing and file sharing, network-based applications, e-mail, personal web publishing space. The Department Chair, Director, or hiring authority must initiate and submit a request for an employee computer account to the Florida State College Learner Support Center. The Acceptable Use Policy governs the use of computer resources and services.

Unique user-ID and passwords are required for each employee. Generic user-IDs based on job function are prohibited. User-IDs must uniquely identify specific individuals. All user-IDs are eight characters or less. A single unique user-ID is used an all platforms (UNIX, Windows, etc.) where authenticated access is required. Naming standards for employee user-IDs is based on the first character of the first name followed by the first seven characters of the last name. If necessary in order to make the user-ID unique, other combinations may be used.

In order to minimize the threat of compromise, the following account policies will be enforced:

- Password length minimum of 8 alphanumeric characters (mixture of lower, upper, and numerics)
- Password will expire after 60 days
- Passwords must be unique and cannot be reused
- Person must change password at initial login after a password creation or reset
- Accounts are locked for five minutes upon three incorrect login attempts
- Timeout for more than 30 minute idle time on any system
- Minimum age of password is 5 days
- All employees are required to enroll in the self-service Password Reset system

You can enroll in the Password Reset System at the following link: http://password.fscj.edu, or from the Artemis homepage under "Account Recovery Enrollment", in the Quick Links area on the left-hand side.

If you would like additional information regarding this service, there is an article and tutorial available on the Techteam website.

Passwords must not be stored in a manner or place where unauthorized persons might gain access to them. Passwords must never be shared or revealed to anyone. The account owner is responsible for any and all actions linked with their user-ID and password.

It is the responsibility of the Department Chair, Director, or original hiring authority to notify Human Resources of dates and times of terminating personnel and termination dates of contractors. This procedure is required to help insure proper auditing and removal of respective systems access accounts. Retiring faculty and staff may be provided an id at retiree@fscj.edu account access limited to the electronic mail system and Internet. Requests for retiree accounts must be made to Human Resources.

Students and Lifetime Members

Any enrolled student may activate a free student computing account to be utilized for academic pursuits while attending Florida State College. A student account is required to gain centralized, authenticated access to basic network resources including, network printing and file sharing, network-based applications, e-mail, courseware systems, personal web publishing space. The Acceptable Use Policy governs the use of computer resources and services.

Unique user-ID and passwords are required for each student. User-IDs must uniquely identify specific individuals. All future student user-IDs will be eight characters and will be a non-descript ID consisting of letters and numbers. A single unique user-ID is used an all platforms (UNIX, Windows, etc.) where authenticated access is required. Persons will not be allowed to change the student IDs issues in the future, for any reason.

In order to minimize the threat of compromise, the following account policies will be enforced:

- Password length minimum of alphanumeric characters (mixture of lower, upper, and numeric)

- Password minimum length must be at least 8 characters and no more than 16 characters
- Passwords must be unique and cannot be reused
- Person must change password at initial login after a password creation or reset
- Timeout for more than one hour idle time on any system

Passwords must not be stored in a manner or place where unauthorized persons might gain access to them. Passwords must never be shared or revealed to anyone. The account owner is responsible for any and all actions linked with their user-ID and password.

Student computing accounts will be active for a minimum of one year beyond the student's last active enrollment period. After 12 months of non-enrollment, student accounts may be deleted in order to regain computing resources.

13-07.13 • DIGITAL SIGNATURES [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this Technology Policy and Procedure is to provide information regarding the use of digital signatures within Information Technology Department.

Description/Procedure:

Applicable Federal and State laws govern the framework for the use and potential use of digital signatures at the College. The implementation of the Electronic Signatures in Global and National Commerce Act ("E-SIGN") (Public Law 106-229) enacted on June 30, 2000. E-SIGN eliminates legal barriers to the use of electronic technology to form and sign contracts, collect and store documents, and send and receive notices and disclosures. Under E-SIGN, companies can contract online to buy and sell a broad array of products and services. E-SIGN eliminates barriers to electronic commerce, while also providing consumers with protections equivalent to those available in the world of paper-based transactions. The Act makes clear that no person is required to use electronic records, signatures, or contracts. Indeed, E-SIGN requires that a consumer affirmatively consent to the use of electronic notices and records. Prior to consenting, the consumer must receive notice of his or her rights. Moreover, the consumer must provide the affirmative consent electronically, in a manner that reasonably demonstrates that the consumer can access the electronic records that are the subject of the consent.

E-SIGN applies broadly to Federal and state statutes and regulations governing private sector (including business-to-business and business-to-consumer) activities. The Act generally covers legal requirements that information be disclosed in private transactions. It also requires that agencies generally permit private parties to retain records electronically. The government may establish appropriate performance standards for the accuracy, integrity, and accessibility of records retained electronically, to ensure compliance with applicable laws and to guard against fraud.

At the State level, the Florida Legislature created the Uniform Electronic Transactions Act (2000 Florida Senate Bill 1334) "UETA". This procedural act established the framework for enforceable electronic contracts and valid electronic signatures to govern electronic records and electronic signatures relating to specified transactions. UETA specifically provides that a record or signature may not be denied legal effect or enforceability solely because it is in electronic form. If a law requires that a signature be notarized, the requirement is satisfied with respect to an electronic signature if an electronic record includes, in addition to the electronic signature to be notarized, the electronic signature of a notary public together with all other information required to be included in a notarization by other applicable law.

13-08.13 • USER AGREEMENT [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The intent of this section is to outline the Information Technology Department's computing services user agreement.

Description/Procedure:

In making appropriate use of Florida State College information resources all students, faculty and staff are required to:

- Protect your User-ID from unauthorized use. You are responsible for all activities initiated under your User-ID.
- Access only files and data that are your own, that are publicly available, or to which you have been given authorized access.
- Be considerate in your use of shared resources. Refrain from monopolizing systems or overloading networks or systems with excessive data.

In making appropriate use of information resources all students, faculty and staff agree not to:

- Use another person's user-ID and password.
- Use another person's files or data without permission.
- Use computer programs to decode passwords or access control information.
- Engage in any activity that might be harmful to systems or to any information stored therein, such as creating or propagating viruses, disrupting services, or damaging files.
- Make or use illegal copies of copyrighted software or other copyrighted material, store such copies on College systems, or transmit them over College networks.
- Use mail or message services to harass, intimidate, or otherwise annoy another person.
- Deliberately perform acts that are wasteful of computing resources. These acts include but are not limited to sending mass mailings or initiating or propagating electronic chain letters and creating unnecessary network traffic

- Use Florida State College network resources to gain unauthorized access to remote computers
- Place or install on any College-owned or operated computer system information or software which:
    - Infringes upon the rights of another person;
    - Is abusive, profane, or obscene;
    - Promotes a commercial enterprise or product; or
    - Does not support official college business or educational pursuits.

All computers connected to the college network including remote access (dial-up or VPN) must be protected with approved anti-virus software. The software must be configured to launch into an active state upon startup and remain in an active state while the computer is operating. With the assistance of the Learner Support Center and the campus computer technical support staff, all users are required to keep the anti-virus software and virus definition files on their computers up-to-date.

The User Agreement is subject to the College's Acceptable Use Policy (as published in the College catalog), all Administrative Procedures and Policies (as published in the College's Administrative and Procedures Manual), all Rules of the District Board of Trustees and all applicable state and federals laws governing the use of computers, networks, and associated resources.

13-09.13 • PRIVACY AGREEMENT (WEB) [REIMAN]

Recommended By:Dennis Reiman, AVP, Tech, Associate CIO & CTO

Purpose:

To provide a policy statement regarding privacy for students, faculty and staff using Florida State College at Jacksonville web servers.

Description/Procedure:

The below listed privacy policy shall be present (via linkage) on all web pages accessed by students, faculty and staff at Florida State College at Jacksonville. The privacy agreement shall be derived in accordance with the Buckley Amendment.

The referenced linkage: the College's Internet Privacy Policy.

13-10.13 • HIPPA [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this Technology Policy and Procedure is to describe the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and relate the requirements of the law (PL 104-191) to the College.

Description/Procedure:

The Health Insurance Portability and Accountability Act (HIPAA) was passed into law in 1996 and was intended to improve the efficiency and effectiveness of the health care system by standardizing data exchange for specific administrative and financial transactions, while protecting the security and confidentiality of that information.

Specifically the following areas are addressed:

Concerns that disclosure of patient medical records could result in embarrassment, insurance declination, loss of employment, or failure to be hired in a new job,

Increasing costs of data exchange in an incompatible and often-competing standards environment to exchange administrative and financial data,

Implement processes and systems to reduce fraud.

HIPAA deals with three standards. One standard on administrative issues addresses the efficiency and effectiveness of interchanging electronic data for administrative and financial transactions such as insurance claims and payments, insurance eligibility and enrollment, and premium payments.

Security and privacy are the other two standards. HIPAA requires security of Individual Identifiable Health Information (IIHI) and mandates privacy, security, confidentiality, and controlled and auditable access to IIHI information. This has a MAJOR effect on how staff currently store and allow access to patient data.

Implications of HIPAA

HIPAA requires the College to examine closely how patient and staff information is managed and stored on the computer infrastructure. While it has safeguards to prevent unauthorized users from accessing 'sensitive' information, the College is faced with HIPAA's fundamental requirement that inserts individual (i.e. patient) into the equation with new rights to control their own information. Apart from the right to inspect, amend and correct their confidential health information, patients now have also the right to control what information can be released and to whom. They are also entitled to be informed of historical transactions against their records, including any transfer of data to other individuals or organizations.

It is essential that everyone understand the difference between "privacy" and "security"; you can have very secure systems where privacy is non-existent. Security involves the means to protect information from unauthorized access. Privacy involves control of access to information as dictated by the authorization of the owner of the information and/or the subject of the information (i.e. the patient). Therefore, be aware that implementing processes, procedures and systems to meet only HIPAA's security requirements is not sufficient and will fail any compliance tests.

The privacy standards of the HIPAA outline specific rights for the individual (the patient) regarding their health information and obligations to keepers of the data. These rules would:

Only permit health information to be used and shared easily for treatment, payment and operations for healthcare,

Only allow health information to be disclosed without patient authorization for certain purposes (such as research, public health, and oversight) but only under defined circumstances; Require written authorization for use and disclosure of health information for other purposes;

Create a set of practices to inform patients how their information is used and disclosed, and ensure they have access to information about them; and

Require health plans and providers to maintain administrative and physical safeguards to protect the confidentiality of health information and guard it from unauthorized access.

Under the proposed rule, specified departments/programs would be prohibited from using or disclosing health information except as authorized by the patient or specifically permitted by the regulation. Note that protection for health information would start when information becomes electronic either by being sent electronically in a specified transaction, or by being maintained in a computer system. Printed copies of electronic information are also protected under the new rule.

At this point it is important to note that these protections are mandated if the information identifies a specific individual. This means that it is OK to use de-identified health information in any way we choose, as long as identifiers have been "stripped" and a key is not disclosed that would allow the information to be re-identified.

College responsibility in complying with HIPAA

HIPAA must be observed in higher education anywhere that personally identifiable patient information is stored or transmitted. These obviously include clinical and hospital records such as those involved in health career programs:

- Secure all medical records from unauthorized access even amongst our own employees.
- Adopt policies, procedures, controls, audit trails and systems which will assure medical data will not be revealed or disclosed for any purpose other than payment and treatment without the express "written" consent of the patient.
- Provide strong authentication for all access, transfer or movement of medical information.
- Make certain that information being disclosed in any manner is not in violation of patient consent.
- Log all access, transfers and use of patient data, including for backup purposes and audit those accesses transfers and uses against patient authorization.

HIPAA affects the College in its health insurance claims and Human Resources. If employees are able to file claims through HR, then claims information must be held confidential. In that the College is self-insured and uses a third-party administrator, then enrollment and disenrollment information is protected under HIPAA legislation. General information pertaining to the legislation can be found at http://www.hhs.gov/ocr/hipaa/.

Technology Division Operations Impact

Just HIPAA's security mandate alone will have a significant impact on our daily operations. For starters, think of all the local databases you may have on your file servers that contain IIHI. You are faced with several issues such as data security, data integrity, virus protection, back up, off site storage, access control, access administration, programming controls, media storage, workstation security, data transmission including e-mail, and authentication. HIPAA calls for:

- Documented formal procedures for selecting and executing security measures;
- Physical safeguards to protect computer systems and other pertinent equipment from fire, other hazards, and intrusion;
- Processes to protect, control and monitor access to the information; and,
- Processes to prevent unauthorized access to the data when transmitted over communication networks or when data physically moves from one location to another using media such as magnetic tape, removable disks or CD media.

Responsibility for implementation and compliance of HIPAA regulations are contained within the functional areas of the College is as follow:

Functional Area	**Requirement/Responsibility**
Health Insurance Information	Human Resources
Dental Clinics	Dean of Workforce – North Campus
Applications	Director of Information Systems
Technology Operations	Security
Database Administration	Director of Information Systems
Financial Aid	Director of Financial Aid

13-11.13 • FERPA [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this Technology Policy and Procedure is to describe the Family Educational Rights and Privacy Act (FERPA) of 1976 (P.L. 93-568, Sec. 2), and relate the requirements as they impact upon the College.

Description/Procedure:

The Family Educational Rights and Privacy Act (FERPA) was passed into law in 1976 and governs: (1) release of records (known as education records) maintained by an educational institution and (2) access to records. This law applies to K-12 as well as post-secondary education. General information pertaining to the legislation can be found at http://www.ed.gov/policy/gen/guid/fpco/ferpa/leg-history.html.

Specifically the following areas are addressed:

- Protection of students' rights to inspect and review their education records.
- Maintenance of records of requests for and disclosures of student education records information
- Protection of students' rights to request to amend their education records.
- Protection of students' rights to limit disclosure of personally identifiable information contained in education records.
- Assurance that third parties do not disclose personally identifiable information except as provided for in the law.

FERPA and Technology

As we move toward an environment with less paper, it is important to note that the same principles of confidentiality must be applied to all media, including but not limited to electronic data, e-mail, and video- or audio-tapes

Technology Division Operations Impact

FERPA's security mandate has a significant effect impact on daily operations. Local databases and file servers that contain student records involve issues such as data security, data integrity, virus protection, back up, off site storage, access control, access administration, programming controls, media storage, workstation security, data transmission including e-mail, and authentication. FERPA calls for:

- Documented formal procedures for selecting and executing security measures;
- Physical safeguards to protect computer systems and other pertinent equipment from fire, other hazards, and intrusion;
- Processes to protect, control and monitor access to the information; and,
- Processes to prevent unauthorized access to the data when transmitted over communication networks or when data physically moves from one location to another using media such as magnetic tape, removable disks or other media.

Dealing with confidentiality requires that audit mechanisms be in place to record and examine any access to student data.

Responsibility for implementation and compliance of FERPA regulations are contained within the functional areas of the College are as follows:

Functional Area	**Requirement/Responsibility**
Student Success Areas	Campus Deans
Counseling	Campus Counselors
Student Records	Registrar
Registrar/Registration	Admissions
Programs which maintain student records	Health Care Programs
Applications	Director of Information Systems
Database Administration	Director of Information Systems
Network Security	AVP for Technology Operation
Financial Aid	Director of Financial Aid

13-12.13 • INCIDENT REPORTING PROCESS [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this Technology Procedure is to identify the incident reporting process for the breech of hardware and/or software security, which may (but not limited to) compromise the safety and privacy of students, faculty, staff, property, or information. It is imperative that all such incidences whether internal or external, be formally reported.

Description/Procedure:

To insure network/electronic data security, users of information technology (IT) devices owned by Florida State College or connected to the College network must report all electronic security incidents promptly to the Computer Incident Response Team (CIRT). The CIRT will be made up of the CIO, technology division staff and administration, security staff, and human resource personnel.

A **Security incident** is any action originating from within the College network or from an outside entity, meeting one or more of the following conditions:

- Any potential violation of federal, state, or local law or College policy involving College Information Technology assets.
- A breach or attempted breach of a Florida State College Information Technology Asset. Security breach or incident includes, but not limited to, the following: Unauthorized access attempts (hacking); Internal or external reconnaissance through probing software (network and port scanning); Denial of Service attacks; Web site defacement; Theft, misuse or critical loss of Technology Division resources including equipment, system information or login identities/passwords; Work practices that do not comply with policy or accepted codes of practice; SPAM e-mail containing unmanaged malicious content or attachments; Threats, harassment, obscene or offensive electronic messages other than SPAM; Unexplained and unusually excessive bandwidth consumption; Other related suspicious activities, events or situations.

- Any unauthorized access or attempt to copy, use, alter or corrupt any Florida State College owned or operated Information Technology Resource (hardware or software) in a manner inconsistent with College policy.
- Any Internet worms, viruses or malicious code.
- Any conduct using any form of Florida State College Technology asset which could be construed as harassing, or in violation of College Policies.
- Any external attack originating on or delivered via any Florida State College owned equipment.

Procedure for Reporting a Security Incident

The Learner Support Center should be notified without delay of any suspected or actual security incident involving College IT Assets. The Learner Support Center will then give further instructions and notify the CIRT. It is crucial that only CIRT personnel take any investigative action.

- When faced with a potential situation, which involves a compromised computer system, the HelpDesk will instruct the caller to do the following:
- Immediately remove the computer from the network.
- Leave the computer system on and all programs currently running are to remain as is. Do not close any programs currently running or shutdown/restart the computer.
- Guard the computer against physical tampering or use.
- Document any information you know while waiting for CIRT to respond to the incident. This may include date, time, and a description of the incident. Any information provided will assist in the investigation.
- Do not speak to anyone other than the CIRT about the incident.

Actions by CIRT:

- If the incident violates federal, state, or local laws, CIRT will contact and work with law enforcement agencies as necessary to help resolve the incident.

- Any other IT security incident, CIRT will act quickly to conduct an assessment and determine the appropriate action.

13-13.13 • WIRELESS ACCESS [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this policy is to limit the installation and maintenance of wireless access points to the Technology Division, and to provide the policies governing client use of Florida State College at Jacksonville's wireless network.

The overriding goal of this policy is to protect Florida State College at Jacksonville's technology-based resources (such as enterprise data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public image. Therefore, all users employing wireless methods of accessing enterprise technology resources must adhere to college-defined processes for doing so, using company-approved access points.

Scope:

This policy applies to all Florida State College at Jacksonville employees, (including full-time staff, part-time staff, contractors, and freelancers), students, and other agents who utilize mobile computers to access the organization's data and networks via wireless means. Wireless access to enterprise network resources is a privilege, not a right. Consequently, employment or enrollment at Florida State College at Jacksonville does not automatically guarantee the granting of wireless access privileges.

This policy is complementary to any previously implemented policies dealing specifically with network access and remote access to the enterprise network.

Access Points:

Florida State College at Jacksonville is committed to providing authorized users with wireless access to the Internet, Florida State College at Jacksonville networks and systems, as well as other enterprise resources. In order to make this convenient service available to end users, the Technology Division will install "access points" in and around the premises wherever wireless access to college resources is designated. These access points are generally small, antenna-equipped boxes that connect directly to the local area network (LAN), converting the LAN's digital signals into radio signals. The radio signals are sent to the network interface card (NIC) of the mobile device (e.g. PDA, laptop, etc.), which then converts the radio signal back to a digital format the mobile device can use.

- As the demand for wireless connectivity increases, so too does the danger of "rogue" access points being surreptitiously installed. Rogue access points are antennas that are installed without the knowledge or permission of the Director of Networks and Telecommunications, used by hackers, internal employees, or trespassers to gain illegal access to the company network and Internet connection for the purposes of sabotage, spamming, corporate espionage, personal gain, and so on.
- All wireless access points within the college firewall will be centrally managed by Florida State College at Jacksonville's Technology Division and will utilize encryption, strong authentication, and other security methods at I.T.'s discretion. Addition of new wireless access points within college facilities will be managed at the sole discretion of Technology Division. A non-sanctioned installation of wireless equipment, or use of unauthorized equipment within the organizational premises, is strictly forbidden.

Policy Restrictions:

5. Florida State College at Jacksonville utilizes the 802.12 b/g/n protocol as its wireless network standard, transmitting at the 2.4 GHz radio frequency spectrums, with the intention of delivering speeds of up to 150 Mbps to mobile and wireless devices.
6. Florida State College at Jacksonville's Technology Division will support only the following devices and equipment for accessing corporate networks and systems wirelessly:
    - Approved Cisco Systems Access Points.

- Client Wireless Access Cards that support 802.12x utilizing the latest Windows or Macintosh operating systems for employees
- Client Wireless Access Cards for the latest Windows and Macintosh desktop operating systems for students.
- Cisco 792x Wireless IP Phones for college employees.
- PDA & Smart Phone Devices for college employees.

7. Florida State College at Jacksonville's Technology Division will strive to purchase only Cisco Systems Access Points 1200 series, or higher, access points and equipment that possess the following characteristics and/or features:
   - RADIUS authentication.
   - SNMP.
   - Syslog.
   - WPA encryption or 802.12x & 802.12i compliant.
   - 128 bit WEP
   - Multi SSID/VLAN support
   - Power-over-Ethernet (PoE).
   - 802.12g signaling and backward-compliant with 802.12b
   - High plenum rating, fire-resistant.
   - Wide temperature range for outdoor use.
8. All wireless clients and devices shall be equipped with host-based personal firewall and anti-virus software. The user shall update these applications as required, and will not reconfigure them in any way.
9. Whenever necessary, the Technology Department will conduct a site survey to determine the appropriate placement of new or additional access points. All installations will be in compliance with all local safety, building, and fire codes.
10. All wireless access points, including those designated for networking home offices or satellite offices with the college network, must be approved by Florida State College at Jacksonville's Associate Vice President - Technology Operations.

11. All access point broadcast frequencies and channels shall be set and maintained by the Technology Department. Any device or equipment found to be interfering with access point signals might be subject to relocation or removal, including cordless phones, microwave ovens, etc.
12. Use of the wireless network is subject to the same guidelines as Florida State College at Jacksonville's technology and Internet acceptable use policies.
13. All enterprise data that traverses the corporate wireless network must be encrypted, The Technology Department will procure only WLAN equipment that supports the chosen encryption method, and will also provide suitable software for authentication and encryption.
14. Florida State College at Jacksonville's Technology Department cannot guarantee 100 percent availability of the wireless network, especially during inclement weather. Nevertheless, the Technology Department will make all possible network adjustments within the supported radio frequency spectrum.
15. The Technology Department will conduct sweeps of the wireless network, using a central wireless management product and hand held wireless sniffers to ensure there are no rogue access points present. Empty rooms and offices will also have all network jacks disconnected from the switch in order to mitigate rogue access point installation.
16. The Technology Department reserves the right to turn off without notice any access point connected to the network that it feels puts the college's systems, data, users, and clients at risk.
17. The wireless access user agrees to immediately report to his/her manager and Florida State College at Jacksonville's Technology Department any incident or suspected incidents of unauthorized access point installation and/or disclosure of company resources, databases, networks, and any other related components of the organization's technology infrastructure.
18. Any questions relating to this policy, as well as any help desk inquiries, should be directed to the Helpdesk at 632-3151 at Florida State College at Jacksonville.edu.

Policy Non-Compliance:

Failure to comply with the Wireless Access Point Policy and subsequent agreement may result in the suspension of remote access privileges, and disciplinary action.

13-14.13 • EMAIL POLICY [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this Technology Policy and Procedure is to clarify appropriate Email storage, volume, and retention periods as well as conventions for the assignment of account names and connection methods.

Description/Procedure:

I. Use of E-Mail

Florida State College at Jacksonville ("College") employees should continue to use the College's computing facilities, including College e-mail, in compliance with Florida State College at Jacksonville's Computing Facilities Policies and User Agreement [Found here: http://www.fscj.edu/district/policies-procedures/acceptable-use/index.php].

The College's e-mail system is provided to employees for official College business. E-mail may be used to communicate with College staff and with other public and private entities to conduct official College business.

Incidental, personal use of the e-mail system is permitted. However, the personal use must be brief, must not interfere with the employee's work or the work of others, must not subject the College to any additional cost, and must not be prohibited by this policy or any federal, state or local law, statute, ordinance, rule or regulation.

Email Accounts are provided to staff, students, and approved contractors. The account names, possible connection methods, and storage policies may differ for each individual account type.

General information for all types of accounts: While some amount of personal email in college accounts is inevitable, excessive volume and/or storage of personal email is strongly discouraged, Email accounts are not to be used as a storage place for databases, pictures,

movies, photos, music, software, or similar items. All users should regularly empty the Deleted Items folder, review the Sent Items folders for unnecessary items, and delete them. Technology Department staff reserve the right to set Automatic Email Policies to remove older messages in various folders as identified in the retention limits for each. Deleted Items will be automatically purged after 6 months, Sent Items will be purged after 1 year, and all other email will be purged after a 2 year time period. The Technology Division does, in the normal course of email support, access email files and folders, account information, attachments, and related items. Additionally, IT provides files and analysis of email, computer accounts, and related information as requested by the College administration and/or authorized investigatory bodies.

Staff is identified as domainID@fscj.edu. Staff may connect to the mail servers in a variety of ways. The supported methods include using the Microsoft Outlook client, Apple Outlook client, and web access through https://webmail.fscj.edu. Staff accounts are deactivated upon termination or resignation. Adjunct faculty may have their accounts deactivated after having not logged-in for a period of 1 year. Supervisors may request alias access to staff accounts for a temporary period in order to retrieve information that may be important to the organization. Deactivated accounts may be removed after 3 months. Staff mailboxes are to remain under 1GB. Warnings will be sent when the mailbox exceeds 800MB. Once a mailbox reaches 900MB, the account will not be allowed to send messages. Once a mailbox reaches 1GB, the account will not be allowed to send or receive further emails. Deleted Items will be automatically purged after 1 month.

Contractors may be identified as domainID@fscj.edu or domainID@project.fscj.edu, based on the purpose and number of IDs requested. Contractors may connect to the mail servers in a variety of ways. The supported methods include using the Microsoft Outlook client, Apple Outlook client, and web access through https://webmail.fscj.edu. Supervisors may request alias access to these accounts for a temporary period in order to retrieve information that may be important to the organization. Contractor mailboxes are to remain under 500MB. Warnings will be sent when the mailbox exceeds 400MB. Once a mailbox reaches 450MB, the account will not be allowed to send messages. Once a mailbox reaches 500MB, the

account will not be allowed to send or receive further emails. Deleted Items will be automatically purged after 3 months.

Students are identified as studentID@students.fscj.edu. This account will be used for Florida State College's communication with the student, including internal courseware communications. Students may connect to the mail servers through Connections. Students that have not been enrolled for one year may be deactivated. Deactivated accounts may be removed after 3 months. Student email is hosted by Microsoft and is subject to Microsoft's Terms and conditions.

II. Prohibitive Use of E-mail

The College's e-mail system shall not be used for any unauthorized purpose including, but not limited to:

A. Sending solicitations including, but not limited to, advertising the sale of goods or services or other commercial activities, which have not been approved by the College.

B. Sending copies of documents in violation of copyright laws or licensing agreements.

C. Sending information or material prohibited or restricted by government security laws or regulations.

D. Sending information or material which may reflect unfavorably on the College or adversely affect the College's ability to carry out its mission.

E. Sending information or material which may be perceived as representing the College's official position on any matter when authority to disseminate such information has not been expressly granted.

F. Sending confidential or proprietary information or data to persons not authorized to receive such information, either within or outside the College.

G. Sending messages or requesting information or material that is fraudulent, harassing, obscene, offensive, discriminatory, lewd, sexually suggestive, sexually explicit,

pornographic, intimidating, defamatory, derogatory, violent or which contains profanity or vulgarity, regardless of intent. Among those which are considered offensive include, but are not limited to, messages containing jokes, slurs, epithets, pictures, caricatures, or other material demonstrating animosity, hatred, disdain, or contempt for a person or group of people because of race, color, age, national origin, gender, religious, or political beliefs, marital status, disability, sexual orientation or any other classification protected by law.

H. Sending messages or requesting information reflecting or containing chain letters.

III. Email as a Public Record

A. What is a Public Record:

College is subject to the Chapter 119, Florida Statutes, Florida's Public Records Law. Florida's Public Records Law defines public records as:

"All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software or other material, regardless of physical form, or characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency." F.S. 119.011(12)

In general, all materials made or received by the College, in connection with official business, which are used to perpetuate, communicate or formalize knowledge, are public records. The law requires the College to retain all public records for an appropriate retention period, as described in Department of State's General Records Schedules. Further, all public records are open for public inspection and/or copying, unless the record is specifically exempted by law. A person need not have a legitimate need for public records to be entitled to inspect them.

B. E-mail as a Public Record:

E-mail created or received by College employees in connection with official business, which perpetuates, communicates, or formalizes knowledge, is subject to the public

records law and open for inspection. Each e-mail's content and purpose, not the form, dictates whether it is a public record. Further, using e-mail (or other electronic messaging) accounts other than those provided by the College does not remove the record from the provisions of Florida's Public Records Law, assuming it is in connection with the transaction of official business by the College.

E-mails created or received for personal use are not generally considered public records and do not fall within the definition of public records by virtue of their placement on a College's computer system. However, if College discovers misuse of their electronic communications system and personal electronic messages are identified as being in violation of the agency's policy, the electronic messages may become public record as part of an investigation.

C. Exemptions to Public Record Law:

State and Federal law exempts certain categories of documents from disclosure under the Public Records Law. The exemptions which apply most often to college records include:

Certain documents involving personnel matters, which are confidential under Florida law;

- Student records which, except for "directory information," must be kept confidential pursuant to the Family Educational Rights and Privacy Act (FERPA); and
- Certain kinds of research records that are confidential under Florida law.
- Before any e-mail is released pursuant to a public records request, any exempt information must be deleted from the e-mail.

D. Responding to a Public Records Request:

Public records requests may be made in writing or orally. The requested department is responsible for contacting the Office of General Counsel to review and assist with the records request prior to release. E-mail that does not fall within the definition of a public

record should not be produced or delivered. E-mail which is a public record but contains exempt information should be produced but the exempt information must first be deleted or redacted.

If the person making the records request wishes to obtain copies of the documents, the public records law allows the College to charge 15 cents per one-sided copy. In addition, if copying the public records requires extensive use of information technology resources or clerical and/or supervisory assistance, the college may assess a reasonable service charge based on the college's actual incurred costs. An estimate of the charges should be given to the requestor and approval obtained prior to responding to the request. All charges should be collected before producing the documents.

IV. Complying with Public Records Law for Email

A. Review Content of E-mail Documents:

All public records must have an approved retention schedule in place before they can be destroyed or otherwise disposed.

Once you have determined an e-mail is a public record and you have stored the e-mail, it be retained for the appropriate amount of time (as described in Department of State's General Records Schedule). For the record series "Electronic Communication," the Department of State's General Records Schedule GS1-SL for State and Local Government Agencies, states:

There is no single retention period that applies to all electronic messages or communications, whether they are sent by e-mail, instant messaging, text messaging (such as SMS, Blackberry PIN, etc), multimedia messaging (such as MMS), chat messaging, social networking (such as Facebook, Twitter, etc.), or any other current or future electronic messaging technology or device. Retention periods are determined by the content, nature, and purpose of records, and are set based on their legal, fiscal, administrative, and historical values, regardless of the format in which they reside or the

method by which they are transmitted. Electronic communications, as with records in other formats, can have a variety of purposes and relate to a variety of program functions and activities. The retention of any particular electronic message will generally be the same as the retention for records in any other format that document the same program function or activity. For instance, electronic communications might fall under a CORRESPONDENCE series, a BUDGET RECORDS series, or one of numerous other series, depending on the content, nature, and purpose of each message. Electronic communications that are created primarily to communicate information of short-term value, such as messages reminding employees about scheduled meetings or appointments, might fall under the "TRANSITORY MESSAGES" series.

Therefore, the retention schedules are based on the e-mail's content, nature and purpose, and are set based on their legal, fiscal, administrative and historical values, regardless of their form. Therefore, there is no single retention schedule that would apply across the board to all e-mails. E-mail, like other records, irrespective of its form, can have a variety of purposes and relate to a variety of program functions and activities. It is the responsibility of each College employee to review the content of each e-mail to determine whether that message may be disposed of or must be retained.

B. Maintaining E-mail Documents:

Public Record e-mails must be retained in accordance with Department of State's General Records Schedule.

While methods for reviewing, storing or deleting e-mail vary, College employees can comply with the retention requirements of Public Records Law by doing either of the following:

1. Electronically store the public record e-mail according to the conventions of your email system and retain it electronically. Each employee's email box contains a folder named "Public Records – 3 Year Retention." Email placed in this folder will be

retained for 3 years and then automatically deleted. If specific records need to be retained longer than 3 years, they should be printed or copied to a different system. Some automatic periodic backup of e-mail by college and department system administrators is done under the college's disaster recovery plan. It is not designed to comply with the public records law. Thus, you need to set up your own retention procedures as outlined above to be sure you are in compliance with the law. An employee may empty their Deleted Items at any time. Items are still recoverable for a short period of time. The Deleted Items folder will be automatically emptied of items that are past one month of being deleted and may be emptied sooner for email systems upgrades and maintenance issues.

OR

2. Print the email and store the hard copy in the relevant subject matter file, as you would any other hard-copy communication. Printouts of e-mail files are acceptable in place of the electronic files provided that the printed version contains all date/time stamps, routing information, etc. This information usually prints automatically at the top of each printed e-mail and includes name of the sender, names of all recipients (including To, CC, and BCC), date/time sent or received, subject line, and an indication if an attachment was present (attachments should be printed and retained with the printed e-mail). This can be applied broadly to other types of electronic records that you are going to print and retain only in paper form. Any metadata that is necessary to understanding the nature and content of the record should be printed along with the record.

However, as indicated in Section V “Litigation Hold on E-mail,” in the event of litigation or reasonably anticipated litigation, existing records in electronic form must be maintained in their current electronic format until all legal discovery issues are closed.

You should consult your department head to determine which retention method is

appropriate. Regardless of the method you decide to use, please remember that the ultimate responsibility for complying with the public records law is on you, the e-mail user.

C. Common E-Mail Retention Schedules

The record schedules described below are provided to assist users in determining retention requirements, and is not designed to be a comprehensive list of all record schedules. [For a more comprehensive list of record schedules, please see: State of Florida General Records Schedule, GS1-SL for State and Local Government Agencies; and State of Florida General Records Schedule, GS5 for Universities and Community Colleges.]

1. Non-Business Communications

E-mails that were not received nor created in the course of College's business do not have to be maintained. Internal and external personal communications or announcements of a non-business nature, and personal notes intended for one's personal use do not need to be retained as public records. These are messages that do not support business purposes. [Please note that the College has established limits on personal use of e-mail, as discussed within this procedure.]

Records Disposal: These e-mails should be deleted and disposed of in a timely manner without the need for any records retention once they no longer have any administrative value, become obsolete, or are superseded. You do not have to document the deletion.

2. Transitory E-mails

Many, but not all, e-mail messages will be transitory e-mails. These e-mail messages have short-lived administrative value and lose that value upon receipt of the communication. These e-mail messages are designed for the informal communication of information and are not designed to formalize or perpetuate information, do not set policy, establish guidelines or procedures, certify a transaction, or become a receipt.

These e-mail messages might be compared to communication taking place during a telephone conversation, verbal communications in an office hallway, telephone voice mail or most written telephone messages. Examples include: reminders to employees about scheduled meetings; most telephone messages; announcements of office events such as holiday parties or group lunches; and receipt copies of office events such as exhibits, lectures, workshops, etc.

Records Disposal: You should delete transitory emails once they no longer have any administrative value, they have become obsolete or they are superseded. You do not have to document the deletion.

3. General Correspondence and Memoranda E-mails

General Correspondence and Memoranda E-mails consist of routine correspondence and memoranda of a general nature that are associated with administrative practices but that do not create policy or procedure, document the business of a particular program, or act as a receipt.

Records Disposal: The sender and receiver should save this e-mail or retain a hard copy for a period of 3 fiscal years, unless it has archival value. If it is not routine correspondence, retain it for as long as the item it relates to. All duplicate copies may be deleted and disposed of in a timely manner once they no longer have any administrative value, become obsolete, or are superseded.

V. Litigation Hold on E-mail

In the case of a litigation hold, all appropriate e-mails, just like every other document, shall be kept, regardless of the record schedule, until the hold is released by the Office of General Counsel.

VI. Frequently Asked Questions:

Q: What do I do when a reporter calls asking for my e-mail?

Notify your department chair or administrative supervisor who will coordinate with the Office of General Counsel the gathering of the public record e-mail documents that need to be given to the reporter.

Q: Does a requestor need to show a "legitimate interest" in my public records e-mail before being allowed to see it?

No. Any person has the right to request to see a public record for any reason.

Q: Does a requestor have the right to conduct a "fishing expedition" and make "overbroad" requests?

Yes. The law does not require the requestor to specify a particular document. You may want to call the Office of General Counsel when responding to "overbroad" requests to seek advice on how to have the request narrowed.

Q: May I refuse to respond to a public records request because I just don't have the time to gather the documents?

No. However, if responding to a public records request requires a substantial amount of time, the law allows you to charge the requestor for the cost of that time.

Q: How do I determine what information is exempt from the public records law?

Contact the Office of General Counsel if you have any questions.

Q: Am I required to produce personal, non-business-related e-mail upon request?

No. Only e-mail made or received pursuant to law or in connection with the transaction of official college business must be produced. Appropriate use of college equipment for personal reasons is addressed in other college policies.

Q: How quickly must I respond to a public records request?

The law requires you to respond within a reasonable time, which will depend on the nature of the request. However, the courts have made it clear that public records are to be given a high priority.

Q: May I require requestors to put public records requests in writing?

No. Oral public records requests are as valid as written requests. However, you may ask for the request to be placed in writing so there are no misunderstandings about what is sought.

Q: Must I produce my public record e-mail in a particular format?

No. You are only required to produce existing records. The law does not require you to create new records.

Q: Does the public records law require me to answer questions regarding the content of public record e-mail?

No. You are only required to produce the documents. You do not have to answer any questions, although at times it may be helpful to do so.

Q: If the person who sent me a public record e-mail asked me to keep it confidential, can I refuse to produce it?

No. If a document is a non-exempt public record, it must be produced upon request, even if the sender has asked that it be kept confidential.

Q: What happens if I refuse to turn over a public record upon request?

A person who knowingly violates the public records law is subject to disciplinary action and may be found guilty of a criminal law violation.

Q: If I keep college public records at my house instead of my office, must I still produce them upon request?

Yes. All non-exempt public records must be produced regardless of where they are physically located.

Q: What if the requested document contains exempt and public material? Can I withhold the entire document?

Not usually. When possible, the law requires you to delete the portion of the document that is exempt and provide the document to the requestor. If this is not possible, the Office of General Counsel can help you comply with the law.

13-15.13 • FLORIDA STATE COLLEGE AT JACKSONVILLE CONTENT FILTERING [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose:

The purpose of this Policy and Procedure is to outline the Internet content filtering solution.

Description:

Florida State College at Jacksonville utilizes a standalone Internet content filtering server appliance that is used to filter pornographic and other inappropriate material.

In addition to pornographic material, Cabinet members may request other services to be filtered for this group of students. While no content filtering method is completely 100% effective, Florida State College's Technology department will provide the best effort possible to prevent access to inappropriate material.

The content filter server appliance determines blocked sites in various ways such as regular library updates from the vendor, manual entry, and keyword entry.

When a client attempts to access a restricted site, they will be redirected to a block page listing the reason why the site was blocked. Because some legitimate sites may mistakenly get blocked, the redirected web page also allows the student to initiate a request to the Technology Department to review the site and removed it from the library of blocked sites.

13-16.13 • WEBSITE DEVELOPMENT: AMERICANS WITH DISABILITIES ACT (ADA) [WICKLINE]

Recommended By: Chrystal Wickline, Multimedia Systems Analyst

Purpose:

The purpose of this section is to describe the standards and regulations regarding the Americans with Disabilities Act (ADA) pertaining to accessible design for all Florida State College websites.

Description/Procedure:

"The Americans with Disabilities Act (ADA) and, if the government entities receive Federal funding, the Rehabilitation Act of 1973, generally require that State and local governments provide qualified individuals with disabilities equal access to their programs, services, or activities unless doing so would fundamentally alter the nature of their programs, services, or activities or would impose an undue burden." (Department of Justice: Civil Rights Division, 2003)

Web accessible sites should provide an equal level of access regarding a variety of options, programs and hours of operation. As an alternative and/or supplement, important documentation such as job announcements, application forms, and the like should be available 24x7 via an information line; although this is not always the most dependable in providing equal degree of access.

Screen readers are used by the blind for image recognition along with other elements of a website/page. Speech devices are used for those persons unable or limited in their mouse mobility. Providing accessible features for people with disabilities also benefits those with older computers and those who use mobile devices.

A resource for web developers and designers is Section 508 Standards of the Information A resource for web developers and designers is at www.access-board.gov and the web-based Intranet and Internet information and applications guide at www.access-board.gov/sec508/guide/1194.22.htm as well a report from the Department of Justice available at www.usdoj.gov/crt/508/report/content.htm.

"Information for web developers interested in making their web pages as accessible as possible, including the current version of the Web Content Accessibility Guidelines (WCAG) Overview (and associated checklists), can be found at www.w3c.org/WAI/Resources, and

Information about the Web Accessibility Initiative can be found at www.w3c.org/WAI." Make sure all new and modified web pages and content are available:

Make sure all new and modified web pages and content are available:

- Images including photos, graphics, scanned images, or image maps, need to include alt tags, captions, and/or long descriptions for each.
- Tables should include header and row identifiers to display information, which relates each data cell by using HTML so the reader can understand the information with a screen reader.
- Documents on a website should be in either HTML or text-based format, [unless client applications for the published document type (such as Acrobat Reader with PDF) meet current accessibility standards].
- Provide a way for visitors to request accessible information or services by posting a telephone number or Email address on your home page.
- Provide a skip navigation link to bypass the row of navigation links so the user can go directly to the start of the web page content. This is useful for screen readers.
- Include a link with contact information for users to request accessible services or to make suggestions.

More Information & Contacts

13-21 • Rehabilitation Act – Section 508 Compliance [Reiman]

"Technical Information Regarding Web Accessibility

For technical assistance regarding Section 508 Standards and how to make web pages accessible to people with disabilities, please contact the Access Board:

- 800-872-2253 (voice)
- 800-993-2822 (TTY)" (Department of Justice: Civil Rights Division, 2003)

Information about the ADA

"The Department of Justice provides technical assistance to help State and local governments understand and comply with the ADA." (Department of Justice: Civil Rights Division, 2003)

ADA Information Line

- 800-514-0301 (voice)
- 800-514-0383 (TTY)
- www.ada.gov

Works Cited

U.S. Department of Justice: Disability Rights Section. (2003, June). Accessibility of State and Local Government Websites to People with Disabilities. (U. D. Justice, Producer) Retrieved September 09, 2008, from Information and Technical Assistance on the Americans with Disabilities Act: http://www.ada.gov/websites2.htm.

13-17.13 • INTERNET DOMAIN REGISTRATION AND CERTIFICATES [SMITH]

Recommended by Ron Smith, AVP, Computing Infrastructure, Security and Compliance & CSO

Purpose:

The purpose of this policy is to provide standards to the purchase, maintenance, administration, and expiration of Internet domains and certificates.

Description/Procedure:

All Internet domain and certificates are to be purchased through the Technology Department and an Engineer will handle the purchase, expiration, renewals, and administration of all domains and certificates.

Marketing will approve any domain requests and expirations. Marketing will periodically review the current list of domains to ensure the need for each.

Wherever possible the Technology Department will purchase all of the common variations of domain names and extensions.

With the exception of .edu domains, all domains will be registered through a single domain registration service and generic accounts will be setup with multiple Engineers and/or AVPs having administration access.

Certificates will be issued based on need and the Technology Department will determine the appropriateness on wildcard or single use certificates based on the application and need.

Domains and certificates issued outside this process are **not** supported by the Technology Department and are **not** considered valid for College business use.

13-18.13 • DRIVE AND MEDIA SANITATION AND DESTRUCTION [SMITH]

Recommended By: Ron Smith, AVP, Computing Infrastructure, Security, Compliance & CSO

Purpose

College staff and faculty often have a business need to store sensitive data on their personal computers. Servers usually contain sensitive information; while student computing resources should never possess prohibited or sensitive data, they do contain license keys for software.

Data sanitization is the process of deliberately, permanently, irreversibly removing, or destroying the data stored on a memory device. The devices discussed below include magnetic disks, flash memory devices, CDs and DVDs, and PDAs and Smart phones. A device that has been sanitized has no usable residual data and even advanced forensic tools will not be able recover sensitive data.

Policy and Procedure

When a staff computer or device is re-assigned for any other purpose the drive is to be sanitized and a new image installed. This ensures security of data and the new use has a clean working set of software applications.

Any college-owned computer device or file server used for staff or student use, is to be properly sanitized with a Department Of Defense level wipe prior to being sent to another organization. Devices slated for surplus are to either be sanitized with a Department Of Defense level wipe or destroyed by a College approved recycler who will certify the proper disposal of the entire device including the sanitation or destruction of the memory.

Phones and portable devices are to have a factory reset performed on them with a clean Operating System or Image installed.

CDs and DVDs with sensitive information are to be shredded. Most paper shredders now have CD/DVD slots to destroy CDs.

USB keys and other storage are to be erased and destroyed.

There are many ways to wipe hard drives and this policy does not specify which method must be used. Below is a list of recommended methods.

The college has an agreement with Creative Recycling, which can shred drives and provide a certificate of destruction.

Apple provides a method to sanitize drives in its Disk Utility. Darik's Boot and Nuke Utility, DBAN (www.dban.org), if free and will handle most types of systems.

13-19.13 • COLLEGE FACT BOOK [LOTT]

Recommended By: Theresa Lott, Executive Director, College Data Reporting

Purpose

The purpose of this procedure shall be to establish responsibilities and guidelines for the annual generation and distribution of the College Fact Book.

Description/Procedure:

The Executive Director, College Data Reporting, shall have the responsibility for the annual generation of the official College Fact Book, as a source of summary, factual information. The book will be published in August of each year, using the certified data from the prior state reporting year as the basis of the information presented.

The College Fact Book shall make available, in one electronic reference, longitudinal information concerning the community served, students, personnel, finances, and facilities of the College.

A section shall be prepared consistent with each of these information categories. The format of the sections of the Fact Book shall provide for the following elements:

- Overview, providing a general discussion of the section's contents and a brief focus regarding the tabular information.
- List of Tables, with reference pages.

The College Fact Book is intended as a local representation of the state-wide Fact Book produced by the Division of Colleges of the Florida Department of Education, and to provide a single reference source for College stakeholders and the public.

The contents of the College Fact Book will be reviewed annually and additional reports, tables, and information may be added if deemed appropriate and useful.

All information will be represented in summary format, with no individually identifiable information included. Where data sets are too small to ensure confidentiality, the data will be perturbed before publication.

13-20.13 • STATE AND FEDERAL REPORTING [LOTT]

Recommended By: Theresa Lott, Executive Director, College Data Reporting

Purpose:

The purpose of this procedure is to present the structure and organization related to the processes governing the reporting of collegewide data to the requisite state and federal entities.

Description/Procedure:

All state and federal data requests originate with the Executive Director of College Data Reporting, who serves as the College liaison with the Florida Department of Education's Division of Florida Colleges, in the role of Reports Coordinator, and with the various federal entities to which the College must report. In addition, the Executive Director serves as a voting member as the College's sole representative on the Management Information Systems Advisory Task Force (MISATFOR).

The Executive Director will disseminate state and federal official communications to the appropriate College data owner. The Executive Director will then work with the data owner(s) to extract data from the official College data systems, to populate report templates and/or create data "flat" files in the official format, to verify and validate that the data in the report is true and correct, to update or enhance existing business processes and the college application systems to reduce or eliminate errors in reporting, to obtain the signature of the College President (or official designee, in the President's absence) as required on data certification forms, and to submit the data, report, and/or certification forms before the stated deadline.

During each reporting cycle, the Executive Director will facilitate review and approval of all data and information used for the state and federal reporting, including dissemination of verification reports to appropriate data owners for their review.

The responsible party for each reporting area is as follows. This responsibility includes ownership of the related data and business processes, verification and validation of extracted data for reporting, and final affirmation for submission of data and/or reports to the state and federal entities. Some responsibilities must be shared, as with the Integrated Database, since the data crosschecks across all databases. This list is dynamic and not intended to be all-inclusive.

Area	Responsible Party	Database or Report
Student	Registrar	Student Database (SDB)
Student	Registrar	Admissions Database (ADB)
Student	Registrar	Integrated Database (IDB)
Student	Registrar	FTE
Student	Registrar	IPEDS Fall Enrollment Survey
Student	Registrar	IPEDS Institutional Characteristics
Student	Registrar	IPEDS Completions Survey
Student	Registrar	IPEDS 12-Month Enrollment Survey
Student	Registrar	IPEDS Graduation Rates
Student	Registrar	Peterson's Guide Survey
Student	Registrar	Rec & Leisure Headcount Report
Student	Registrar	Accountability
Student	Registrar	Anticipated Degree Graduates
Student	Director of Financial Aid	IPEDS Financial Aid Survey
Student	Director of Financial Aid	Annual Financial Aid Database (RT8)
Student	Director of Financial Aid	USDOE Gainful Employment
Student	Director of Financial Aid	Federal Net Price Calculator
Student	Director of Recruitment	College Board Survey
Student	AVP, Degree and Career Programs	AA/AS Level II Report
Student	AVP, Degree and Career Programs	Level II Vocational Program Review
Student	AVP, Degree and Career Programs	Accountability
Student	AVP, Degree and Career Programs	Concurrent and Joint-Use Report
Student	AVP, Degree and Career Programs	USDOE Gainful Employment

Student	AVP, Liberal Arts and Sciences	AA/AS Level II Report
Student	AVP, Liberal Arts and Sciences	Accountability
Student	AVP, Liberal Arts and Sciences	Concurrent and Joint-Use Report
Student	Dean of Pre-Collegiate Studies	National Reporting System (NRS)
Student	Dean of Pre-Collegiate Studies	Request for GED File
Student	Director of Students with Disabilities	Report of Actual Services and Expenditures to Support Students with Disabilities
Student	Director of Students with Disabilities	Students with Disabilities Report
Facilities	AVP, Facilities Management and Construction	Office of Educational Facilities Reports, collectively
Facilities	AVP, Facilities Management and Construction	State Board of Education Capital Outlay Bonds (SCOA-1)
Facilities	AVP, Facilities Management and Construction	Operating Cost of New Facilities
Facilities	AVP, Facilities Management and Construction	Educational Plant Survey
Facilities	AVP, Facilities Management and Construction	Plant Safety Report
Facilities	AVP, Facilities Management and Construction	New Site Inspection
Facilities	AVP, Facilities Management and Construction	Local Safety Report
Facilities	AVP, Facilities Management and Construction	Non-PECO Initial Request
Facilities	AVP, Facilities Management and Construction	Facility Enhancement Challenge Grant (FECGP-1)
Facilities	Planning Specialist	Facilities and Capital Outlay Database (FCODB)
Facilities	Planning Specialist	Integrated Database (IDB)
HR	Human Resource Information Manager	Personnel Database (PDB)
HR	Human Resource Information Manager	Annual Personnel Report (APR) and Fringe Benefits Report
HR	Human Resource Information Manager	Integrated Database
HR	Human Resource Information Manager	IPEDS Human Resources Survey
HR	Human Resource Information Manager	CC Directory
Finance	VP of Administrative Services	FTE Enrollment Plan

Finance	VP of Administrative Services	Dr. Benjamin Estimate and Report
Finance	VP of Administrative Services	Capital Improvement Program (CIP)
Finance	VP of Administrative Services	Workforce Financial Aid Fee Report
Finance	VP of Administrative Services	Direct Support Organizations
Finance	VP of Administrative Services	Report on Estimated Actual CO & DS Instructional Units
Finance	AVP of Financial Services	Personnel Database (PDB)
Finance	AVP of Financial Services	Annual Personnel Report (APR) and Fringe Benefits Report
Finance	AVP of Financial Services	Integrated Database (IDB)
Finance	AVP of Financial Services	Annual Financial Report (AFR)
Finance	AVP of Financial Services	Cost Analysis Report
Finance	AVP of Financial Services	IPEDS Finance Survey
Finance	AVP of Financial Services	College Operating Budget
Finance	Director of Risk Management, Environmental and Fire Safety	Crime Statistics Survey
General Counsel	Director of Policy and Compliance	College Annual Equity Report
Purchasing	AVP, Purchasing and Business Services	Minority Business Expenditures Quarterly Report (MBE)
Learning Resources	Library Tech Services Manager	NCES Academic Library Survey
Curriculum	Curriculum Services Coordinator	Course Match Report (SDB)

Table 13.2: Responsible Parties for Reporting

13-21.13 • REHABILITATION ACT – SECTION 508 COMPLIANCE [REIMAN]

Recommended By: Dennis Reiman, AVP, Technology, Associate CIO & CTO

Purpose

The purpose of this Technology Policy and Procedure is to identify the College's compliance with Section 508 of the Rehabilitation Act of 1973.

Description/Procedure:

The Rehabilitation Act of 1973, Section 508, requires institutions that receive Federal funds to make reasonable efforts to accommodate individuals with disabilities by providing them access to and use of electronic and information technology.

The College continually evaluates electronic and information technology including for compliance with Section 508; where it can be operated in a variety of ways and does not rely on a single sense or ability of the user.

Reference resources:

13-16.12 • Website Development: Americans with Disabilities Act (ADA) [Wickline]

http://www.section508.gov/

http://www.access-board.gov/sec508/guide/1194.22.htm

http://www.justice.gov/crt/508/report/content.php

http://www.w3.org/WAI/Resources/