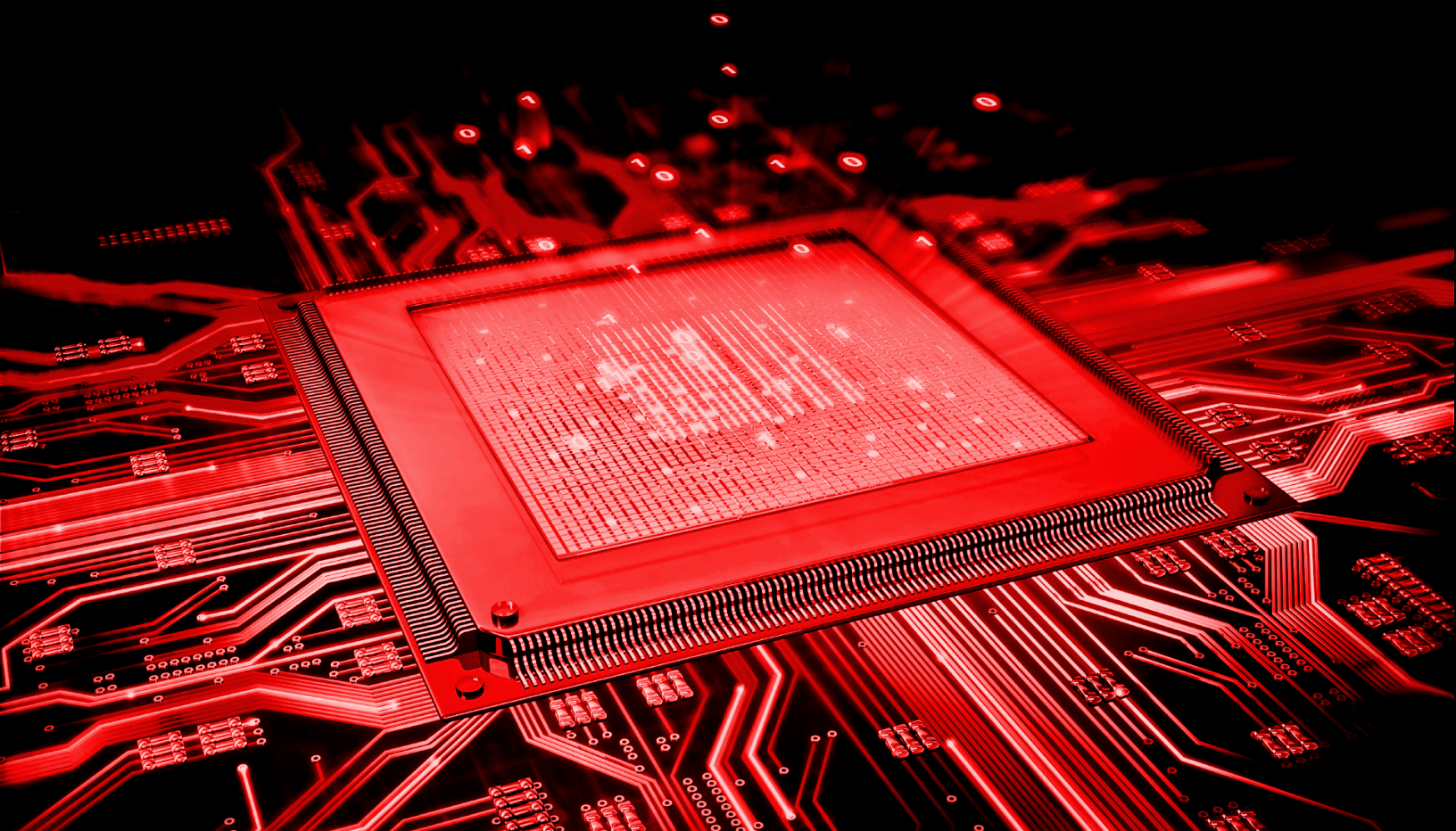
FLORIDA STATE COLLEGE AT JACKSONVILLE™

Information Policies and Procedures

Ron Smith - Chief Information Officer



Documents are reviewed quarterly and updated as necessary

Reviewed & Approved By: Ron Smith, Chief Information Officer

Last Update: February, 2019

IT Organization

01-01 • Technology Vision, Mission, Charge, & Goals

Recommended and Reviewed By: CIO

Last Review Date: February, 2022

Purpose

The purpose of this policy is to present the technology vision, mission, and values of the College as expressed in the technology vision, mission, values, and goals.

Policy:

Mission and Vision

Information Technology at Florida State College at Jacksonville strives to be a service-based, innovative, evolving, creative team. These ideals are expressed professionally and consistently through transparent communication and client-centered excellence in support of teaching and learning.

IT provides leadership, coordination, management and support to the academic and administrative computing activities of Florida State College at Jacksonville. As a service organization, IT works collaboratively across the college community to:

- Digitally connect Florida State College at Jacksonville together locally and globally through information and communication technologies;
- Provide innovative and open technology environments and services where teaching and learning can occur anytime and anyplace;
- Seek out and share the practical applications of the college's technological knowledge and expertise to benefit college students, faculty, and staff;
- Enable and consistently improve Florida State College at Jacksonville's administrative technology to deliver quality education services and outcomes based on data-driven decisions;
- Provide a unified customer experience and service management ecosystem to continuously improve and enable total quality control of the IT service catalog;
- Research and explore new and emerging technologies and tools related to Higher Education in the 21st century in conjunction with college initiatives.

Values

In support of our efforts, the IT organization will affirm the following core values:

- A shared vision;
- An environment of integrity, trust, and open communication;
- An ideal of excellence, fostered by a belief in quality, teamwork and service;
- A spirit of courage and risk-taking that nurtures technological creativity and innovation.

Goals

The Major Goals and Initiatives will be posted in the Strategic Technology Plan and be created in support of the College Mission and Goals.

01-02 General Purpose and Organization

Recommended and Reviewed By: CIO

Last Review Date: February, 2022

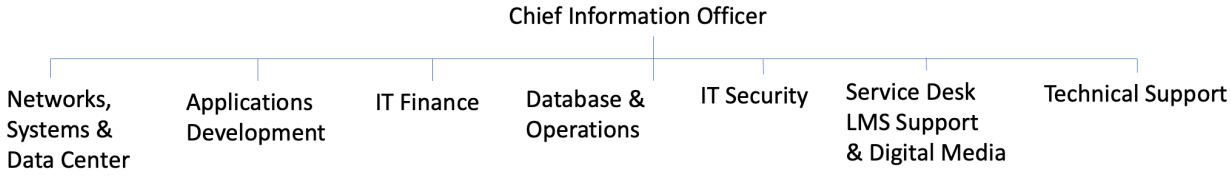
Purpose

The purpose of this policy is to provide the framework for the IT divisional organizational structure and reporting relationships and present a description of the organization principles applied.

Policy

The IT division comprises information systems and technology-related functions of the College. The Chief Information Officer (CIO), heads the IT division. The CIO reports to the Vice President of Business Services.

The CIO designates direct reports and the following is the current composition of the department



01-03 Technology Strategic Planning

Recommended and Reviewed By: CIO
Last Review Date: February, 2022

Purpose

The purpose of this policy is to provide and an overview of the IT strategic planning process and the resultant publication of the College's Strategic Technology Plan.

Policy

The CIO shall work with College leadership to create an agreed upon Strategic Technology Plan that supports the College-wide planning process. Coordination objectives involve establishment and maintenance of formal structures through which various College stakeholders can provide feedback, interact with the Chief Information Officer, and advise on stakeholder needs. Moreover, objectives related to this goal serve to involve College stakeholders in the design, construction, and advancement of technology implementations College-wide. IT Organizational development objectives create an opportunity to build a more informed and innovative technology community within the College.

01-04 College-wide Information Technology Governance Model

Recommended and Reviewed By: CIO

Last Review Date: February, 2022

Purpose

The purpose of this procedure is to describe the role of the College-wide information technology governance model.

Policy

The College-wide information technology governance model is formed and operates under college APMs and is an important element of the governance process for technology.

Objective

Establish a technology community organization structure that supports a functional, collaborative, and dynamic technology community at the College between IT, technology stakeholders, and distributed college IT providers.

Objective Description

Florida State College at Jacksonville stakeholders play a major role in the design, development, and delivery of IT services. As such, stakeholder involvement in establishing priorities, technology planning, risk, policy and best practices, and decision making with respect to the use of academic and administrative technologies. Shared governance involves stakeholder input in three primary College areas: academic computing, administrative computing, and data driven support. The IT governance objective works with two committees, each charged (respectively) with representing the interests and needs in these two areas.

IT Leadership is made up of the leaders of the main IT divisions. Its purpose is to discuss the current and future projects in IT, work together on solutions, and ensure forward progress on initiatives.

The ERP Steering Committee is made up of members of the various departments that rely on the college's ERP system, PeopleSoft. Its purpose it to prioritize upgrades, integrations, development, and the status of ERP-related projects.

The Academic Technology Committee (ATC) a subcommittee of Faculty Senate designed to be a listening post to hear and discuss academic technology issues and needs for students and faculty. The committee is chaired by a Faculty Senate representative. The committee is made up of faculty members, the CIO, and various IT Leadership members.

The Business Services Team represents the College's administrative services. The CIO attends these meetings.

The Data Governance Team is chaired by a member of Institutional Research and is made up of the "data owner" representatives from the different divisions of the college.

01-06 • IT Resource Allocation, Budgeting, and Fiscal Analysis [Thomas]

Recommended and Reviewed By: IT Budget Director
Last Review Date: February, 2022

Purpose

The purpose of this policy and procedure is to describe the resource allocation process for technology within the College. The Technology Department operates within the Board of Trustee Rules, 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.

Policy

The Technology Department formulates technology allocation plans on a yearly basis with input from the College's community representatives (faculty, students, staff, and administration.) Approvals are secured as part of the College's overall annual budget adoption process.

- Technology Resources Allocation
  - Allocation of technology resources for academic purposes, for use by faculty, academic staff, and students under the direction of faculty, are a primary priority within the Technology Department.
  - Allocation of technology resources to academic and administrative functions support the College's goals, priorities, and initiatives for a given year, as well as the College's Strategic Technology Plan.
  - Total technology resources available in a given year vary depending upon State appropriations, funding for special technology-related programs, technology-related grant funding, and college-wide funding decisions.

Procedure

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 (MTI) 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 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
- 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 implemented analytical tools to complement the budget and financial analytical capabilities of the ERP System. Central to these tools is the use of project codes to link departmental budgets and operational and capital expenditures.

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.

01-07 Authority for Technology Desktop Procedures [Smith]

Recommended and Reviewed By: CIO
Last Review Date: February, 2022

Purpose

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

Policy

Florida Statute 240.319 provides for the establishment of policies and procedures/ desktop procedures governing the use of technology resources in state colleges. The College has general Board Rules and APMs regarding technology. The Technology Desktop Procedures Manual serves as the specific operational implementing structure for Board Rules section 6Hx7-7.1 and APM Chapter 07.

01-08 Technology Approval Due Diligence

Recommended and Reviewed By: CIO

Last Review Date: February, 2022

Purpose

The purpose of this policy and procedure is to describe the due diligence process of the Technology Department in the selection and approval of technology solutions.

Policy

The IT division is responsible for performing the due diligence evaluations of technology solutions for the College. The College's CIO is specifically charged with envisioning the efficacy, appropriateness, cost effectiveness, and technology fit of potential solutions prior to approval for acquisition. Technology solutions cover software, certain services, integrated solutions, cloud solutions, and hardware.

The following procedures are internal to the IT division and do not describe approval or due diligence procedures performed outside of the IT division.

The College engages in a robust due diligence process for the selection and acquisition of technology solutions. The CIO serves as the process owner who is charged with developing and monitoring adherence to the due diligence methodology. CIO approval of the selected process and solution must occur prior to acquisition. The College's CIO and other IT executive leaders 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.

Procedure

Software

Beyond the four due diligence factors stated in the policy above, software is evaluated on purpose (academic or administrative), status (already in the *3-Year Master Plan*), location (server, desktop, etc.), distribution, and cost.

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 IT senior 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 IT executive 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. The IT division subjects integrated solutions to the applicable software and hardware acquisition procedures. It is further evaluated based upon optimized decision matrices and requirements gathering in keeping with IIBA and PMI.

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. It is further evaluated based upon optimized decision matrices and requirements gathering in keeping with IIBA and PMI.

Hardware

Reference *Technology Equipment Requirements* for information as it pertains to standards and requirements for hardware acquisition College-wide. 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 documents and are reviewed quarterly and updated as necessary. It is further evaluated based upon optimized decision matrices and requirements gathering in keeping with IIBA and PMI.

Acceptable Use

01-01 • Computer Crimes & Software Piracy [Smith]

Owner: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer

Management: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer

Purpose

The purpose of this 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.

Policy

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. Definitions, general penalties, and registration of criminals is covered in Chapter 775, Florida Statues. Provisions supplemental to criminal procedure law are covered in Chapter 932, Florida Statutes.

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 Applications Specialist, Network Application Specialist, System Administrator, Dean and/or Executive Dean, Campus President, President, and Board of Trustees

Table 01.01: 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 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 to assure compliance with applicable legal requirements and reduce the College's potential liability for violations.

Procedure

Under the direction of the Executive Director, Computing Infrastructure, Security, Compliance, & CSO an annual assessment of compliance is performed and improvements are recommended if necessary.

College employees and faculty shall:

- Be proactive in education about software licensing and copyright
- Keep records of software licenses, POs, shareware receipts, and written permissions for software for machines in the department (The IT department will keep a record of all licenses that are sent to it to prevent future loss of licenses.)
- Have usage written into software licenses when he/she purchase software so that he/she does not have license violations to get his/her job done
-
- Know licenses' content for familiarization of software legality
- Have employees and students sign a statement agreeing to the acceptable use policy.
- Get permission in writing from the vendor for additional use of a software product beyond agreed upon license.
-

AREA	REQUIREMENT/RESPONSIBILITY
CAMPUS LEARNING ASSISTANCE	Learning Assistance Lab Manager, Lead Campus Computer Technician
CENTERS	Lead Campus Computer Technician
CAMPUS COMPUTER LABS	Computer Lab Manager, Lead Campus Computer Technician

AREA	REQUIREMENT/RESPONSIBILITY
PROGRAM SPECIFIC COMPUTER LABS	Program Faculty, Lead Campus Computer Technician
CAMPUS COMPUTING SYSTEMS	Director of Administrative Services, Lead Campus Computer Technician
COLLEGE-WIDE NETWORK SYSTEMS	Executive director of IT
COLLEGE-WIDE COMPLIANCE	Executive director of IT

Table 01.02: Reducing Liability

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

Software & Information Industry Association

www.siia.net

01-02 • Voicemail, Moves, Adds, and Changes (MAC) [Smith]

Owner: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer

Management: Jim Augherton, Network Engineer

Purpose

The purpose of this policy and procedure is to describe the basic guidelines for the College's voicemail system usage and describe the process for Moves, Adds, and Changes (MAC) of the College-wide telephone service.

Policy

FSCJ utilizes a Cisco IP telephone and Cisco Unity voicemail system. Employees shall access their messages routinely and clear his/her 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.

The College utilizes a Cisco IP phone system which, is maintained by FSCJ's Network Infrastructure and Telecommunications Team.

Procedure

A change by an end user to move, add, or change shall be initiated through the college's internal helpdesk ticketing system

01-03 • User Agreement [Smith]

Owner: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer
Management: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer

Purpose

The purpose of this policy and procedure is to outline the Technology Department's computing services user agreement.

Policy

All computers connected to the College network, including remote access connected computers, 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.

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 federal laws governing the use of computers, networks, and associated resources.

Procedure

College employees, faculty, and students shall contact his/her campus computer technical support staff to install and update anti-virus software and virus definition files on his/her computer(s).

All college employees, faculty, and students are required to:

- Protect his/her User-ID from unauthorized use for which he/she is responsible for all activities initiated under his/her User-ID
- Access only files and data that are his/her own, that are publicly available, or to which he/she has been given authorized access
- Be considerate in his/her use of shared resources and refrain from monopolizing systems or overloading networks or systems with excessive data

All college employees, faculty, and students 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 which is harmful to systems or 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 which are wasteful of computing resources, which include but are not limited to: sending mass mailings or initiating or propagating electronic chain letters and creating unnecessary network traffic
- Use FSCJ network resources to gain unauthorized access to remote computers
- Place or install on any FSCJ-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
    - Does not support official college business or educational pursuits

01-05 • Email Policy [Smith]

Owner: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer
Management: Pete Snell Director of Systems Engineering

Purpose

The purpose of this 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.

Policy

Use of E-Mail

FSCJ employees shall continue to use the College's computing facilities, including college email, in compliance with FSCJ's Computing Facilities Policies and User Agreement.

The FSCJ's email system is provided to employees for official college business and email may be used to communicate with college staff and other public/private entities to conduct official college business.

Incidental, personal use of the email system is permitted. However, personal use must be brief, not interfere with employee's work or the work of others, not subject FSCJ to additional cost, and not be prohibited by this policy, 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 account types – While some amount of personal email in college accounts is inevitable, excessive volume and/or storage of personal email is strongly discouraged. Email accounts used as a storage place for databases, pictures, movies, photos, music, software, or similar items is prohibited. Technology Department staff reserve the right to set automatic email policies for removal of messages six months or older from date of receipt in various folders as identified in the retention limits for each. Deleted items are automatically purged after six months, sent items are purged after one year from date of receipt, and all other email is purged after a two-year time period. The Technology Department does, in the normal course of email support, access email files and folders, account information, attachments, and related items. Additionally, the Technology Department provides files and analysis of email, computer accounts, and related information as requested by the College administration and/or authorized investigatory bodies.

Staff email is identified as *domainID@fscj.edu*. Staff may connect to the mail servers in a variety of ways. The supported methods include but are not limited to: 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 his/her accounts deactivated after having not logged-in for a period of one year. Supervisors may request alias access to staff accounts for a temporary period in order to retrieve information important to the organization.

Deactivated accounts may be removed after three months. Deleted items are automatically purged after one month.

Contractors' email is identified as *domainID@fscj.edu* or *domainID@project.fscj.edu*, based on the purpose and number of IDs requested. Contractors can 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 important to the organization.. Deleted items are automatically purged after three months.

Students are identified as *studentID@students.fscj.edu*. This account shall be used for FSCJ communication with the student, including internal courseware communications. Students can access their college provided email through Connections. Students not enrolled for one year may be deactivated. Deactivated accounts are removed after three months. Student email is hosted by Microsoft and is subject to Microsoft's Terms and conditions.

Policy

Prohibitive Use of E-mail

The FSCJ's email system shall not be used for any unauthorized purpose including, but not limited to:

- Sending solicitations including, advertising the sale of goods, services or other commercial activities, not approved by the FSCJ
- Sending copies of documents in violation of copyright laws or licensing agreements
- Sending information or material prohibited or restricted by government security laws or regulations
- Sending information or material which may reflect unfavorably on the College or adversely affect the College's ability to carry out its mission
- 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
- Sending confidential or proprietary information or data to persons not authorized to receive such information, either within or outside the College
- Sending messages, requesting information or material which 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
- Sending messages or requesting information reflecting or containing chain letters

What is a Public Record?

FSCJ is subject to Chapter 119 of the Florida Statutes, Florida's Public Records Law. Section 119.011 Definitions of Florida's Public Records Law defines public records as:

"'"Public records"' means all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, 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.

Email as a Public Record

Email 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 email's content and purpose, not the form, dictates whether it is a public record. Further, using email (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.

Emails 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 the College discovers misuse of its 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.

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)
- Certain kinds of research records that are confidential under Florida law

Before any email is released pursuant to a public records request, any exempt information must be deleted from the email.

Responding to a Public Records Request

Email that does not fall within the definition of a public record should not be produced or delivered. Email 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 is allowed to 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.

Complying with Public Records Law for Email

Review Content of Email Documents

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

Once he/she has determined an email is a public record and he/she has stored the email, it must 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 email's content, nature, and purpose, and are set based on their legal, fiscal, administrative, and historical values, regardless of their form. There is no single retention schedule which would apply across the board to all emails. Email, 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 email to determine whether that message may be disposed of or must be retained.

Maintaining Email Documents

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

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

- Electronically store the public record email according to the conventions of his/her 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 is retained for three years and then automatically deleted. If specific records need to be retained longer than three years, he/she must print or copy to a different system. Some automatic periodic backup of email 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, he/she needs to set up his/her own retention procedures as outlined above to assure he/she is in compliance with the law. An employee may empty their *Deleted Items* at any time in accordance with the *General information for all* section previously mentioned in this policy. Items are still recoverable for a short period of time. The *Deleted Items* folder is 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

- Printing the email and storing the hard copy in the relevant subject matter file, as he/she would any other hard-copy communication. Printouts of email 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 email 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 he/she is printing and retaining 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.

The employee should consult his/her department head to determine which retention method is appropriate. Regardless of the method he/she decides to use, please remember the ultimate responsibility for complying with the public records law is the e-mail user.

Common Email 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.]

Non-Business Communications

Emails 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 email, as discussed within this policy.]

Transitory Emails

Many, but not all, email messages are transitory emails. These email messages have short-lived administrative value and lose value upon receipt of the communication. These email 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 email 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.

General Correspondence and Memoranda Emails

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

Litigation Hold on Email

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

Procedure

Use of E-Mail

- All users are expected to empty his/her Deleted Items folder weekly, review the Sent Items folders for unnecessary items, and delete them
- Requests for access to staff and/or contractor accounts via alias must be submitted to the Technology Department from the requestor's college email

Responding to a Public Records Request

- Public records requests can 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.

Non-Business Communications

Records Disposal

- These emails must 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
- Documenting the deletion is not required

Transitory Emails

Records Disposal

- Transitory emails should be deleted once they no longer have any administrative value, they have become obsolete, or they are superseded
- Documenting the deletion is not required

General Correspondence and Memoranda Emails

Records Disposal

- The sender and receiver should save this email or retain a hard copy for a period of three fiscal years, unless it has archival value
- If it is not routine correspondence, he/she should retain it for as long as the item it relates to
- All duplicate copies can be deleted and disposed of in a timely manner once they no longer have any administrative value, become obsolete, or are superseded

Frequently Asked Questions

Q: What do I do when a reporter calls asking for my email?

Notify the department chair or administrative supervisor who will coordinate with the Office of General Counsel the gathering of the public record email documents to be given to the reporter.

Q: Does a requestor need to show a *legitimate interest* in my public records email 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 *over broad* requests?

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

Q: May an individual refuse to respond to a public records request because he/she doesn'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 the employee to charge the requestor for the cost of his/her time.

Q: How is information exemption determined in the public records law?

Contact the Office of General Counsel for questions.

Q: Is it required to produce personal, non-business-related email upon request?

No. Only email 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 one respond to a public records request?

The law requires the employee to respond within a reasonable time, which will depend on the nature of the request. However, the courts have made it clear public records are to be given a high priority.

Q: May one require requestors to put public records requests in writing?

No. Oral public records requests are as valid as written requests. However, the employee may ask for the request to be placed in writing so there are no misunderstandings about what is sought.

Q: Must public record email requests have a particular format?

No. The only requirement is to produce existing records. The law does not require the creation of new records.

Q: Does the public records law require answering questions regarding the content of public record email?

No. The only requirement is to produce the documents. Questions do not have to be answered, although at times it may be helpful to do so.

Q: If the person who sent a public record email asked the receiver to keep it confidential, can he/she 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 a public record upon request is refused?

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 college public records are kept in personal location instead of an office, must they still be produced 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 the entire document be withheld?

Not usually. When possible, the law requires the deletion of the portion of the document that is exempt and then provide the document to the requestor. If this is not possible, the Office of General Counsel can help with compliance of the law.

01-06.14 Video Surveillance and Monitoring

Owner: Ron Smith, Deputy Chief Techology OfficerManagement: Ron Smith, Executive Director, Infrastructure, Operations, Service Management & CSO

Purpose

The purpose of this policy is define the proper selection, use, installation and monitoring of video surveillance systems.

Policy

The purpose of video surveillance is to provide for the safety and security of students, staff, visitors, and college property. Locations for cameras shall be selected first to deter and detect crimes against persons and, second, to protect college property against theft and vandalism, and for no other purpose. While the IT department will assist on placement planning, it is ultimately the responsibility of the each Campus President's office to determine the installation locations. Cameras shall not be installed as a means to monitor individuals, employees for performance purposes, or in areas that assume general privacy. The only exception is that if cameras are installed for investigative purposes, are hidden, or used to monitor an individual, they must first be approved in writing by the College President. This written authorization will include the specific purpose and period of time that such use is authorized.

While the cameras are for safety and security, there is no guarantee that each individual camera is operational or being observed and recorded at all time periods or that an individual's safety is guaranteed . As such, the installation and use of cameras does not ensure an individual's safety. Cameras are not always in operation or being monitored. All employees, students and visitors to the College should be mindful of their surroundings and take all necessary precautions for their own safety.

Cameras are to adhere to the IT department's Technology Equipment Requirements guide and be installed in accordance to the Technology Construction Requirements Guide.

Safety and security cameras or their housings are to be installed in visible places to maximize their deterrence affect and enable the most effective use of assigned security staff. Cameras may not be visible if they are installed in housings but the housings should be visible. Empty housings, referred to as dummy cams, are allowed to be installed.

The IT department will maintain the college-wide recording system as well as monitor the recordings for security technical spaces. All other cameras will monitored by the respective security departments or persons identified by the campus presidents. The Director of Risk Management should have access to all camera recordings. Campuses and Centers shall provide a list of all their installed cameras to the Director of Risk Management, and updated lists each time a change is made.

Recordings are to be kept for 30 days, as per the State of Florida Records Retention Schedule.

The exception to this policy is with Downtown Campus' camera system. This system is currently autonomous from the rest of the college and managed by personnel at Downtown campus.

In general, video recordings made for security purposes may be released for security and other investigative purposes, such as claims administration or to verify reports of threatening or disruptive behavior, to JSO, other law enforcement, to the College's Director of Risk Management, the College's Equity Officer, the Vice President Administration and other Cabinet members, the Office of the General Counsel, Directors of Administrative Services, Deans of Student Success, and Center Directors. Security may also review video at the request of the general public, other employees, and students, not to interfere with their College duties, for the purposes of identifying the causes of thefts and damage to personal property. This paragraph shall not be construed as authorizing the installation of surveillance for any other reasons than those of security and safety as described above.

01-07 Monitoring and Review of Employee Electronic Communications or Files

Owner: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer Management: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer Purpose

Defines College policy on institutional monitoring or review of the content of employee electronic communications or employee electronic files.

Policy

No user should have any expectation of privacy in any message, file, image or data created, sent, retrieved or received by use of the College's equipment and/or access. The College has the right to monitor any and all aspects of their computer systems at any time, without notice, and without the user's permission. The policy applies to all employees and students.

The College holds as core values the principles of academic freedom and free expression. In consideration of these principles, the College will not monitor the content of electronic communications of its employees in most instances, nor will it examine the content of employee electronic communications or other employee electronic files stored on its systems except under certain circumstances. In this context, "electronic communications" includes telephone communications, so-called "phone mail," e-mail, and computer files traversing the network or stored on College equipment.

Examples of when monitoring and/or review may occur include, but are not limited to, the following circumstances:

¥ communications or files targeted by orders of a court of law or requested as per Florida Public Records law.
¥ supervisor and/or Internal Audit review of College telephone system long-distance call records.
¥ electronic communications or files that have been inadvertently exposed to technical staff who are operating in good faith to resolve technical problems. When technical staff inadvertently see or hear potentially illegal content in communications or files, they are required to report what they have seen or heard to appropriate authorities. Otherwise, the College expects technical staff to treat inadvertently encountered electronic

communications and files of employees and students as confidential and not subject to disclosure to anyone.

¥ routine administrative functions, such as security tests of computing systems, including password testing by system administrators to identify guessable passwords, and investigations of attempted access into systems by unauthorized persons (system administrators and other technical staff will not access employees' electronic communications or files while performing these functions).

¥ situations such as:

◦ an investigation into allegations of violations of law or policy

◦ an urgent need for access to College business documents when an employee is unavailable

¥ Such situations will be specifically reviewed by and approved by the president or the vice president (or equivalent) responsible for the affected employee(s), Human Resources and or Legal Counsel and be handled by the IT departments Compliance Officer.

¥ for some units of the College, routine monitoring or examination of employee electronic communications or files as part of the work environment. Such routines must be approved by the relevant vice president (or equivalent), and affected employees must be informed in advance that such monitoring or examination will be taking place.

This policy does not mean that the College has lower expectations for its employees' behavior. It expects College employees to obey all applicable policies and laws in the use of computing and communications technologies.

This policy shall not be interpreted as requiring public disclosure of confidential and privileged attorney-client communications with the College's Office of General Counsel.

Figure 1

Standards

04-01 • Green IT Policy [Smith]

Recommended and Reviewed By: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer

Management: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer

Purpose

The purpose of this policy and procedure is to define the areas of considerations in the design, and product selection of college-wide technologies in relation to energy efficiency and environmental responsibility.

Policy

The Network Operations Center follows 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, shall be made with energy efficiency in mind. Refresh cycles shall bring in more energy efficient systems and push less efficient systems out of the organization. IT hardware vendors are members of the US Government's Energy Star Program, www.energystar.gov .

The Technology Department and Desktop Support leaders shall 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 are 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 shall be made with waste reduction in mind.

Procedure

Wherever possible:

- Redundant technology services are to be consolidated
- Servers are to be centralized at the Network Operations Center (NOC) at the Deerwood Center
- Applications which do not require full processing potential of their server but do no need their own environment shall be moved to a virtual environment such as a VMWare or Zone architecture

- If manuals and media are not needed for each install, they should not be ordered. The Technology Department 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 are recommended when buying from individual vendors that offer such, in order to reduce the amount of non-recyclable material.

04-02 • Technology Architecture [Smith]

Recommended and Reviewed By: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer

Management: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer

Purpose

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

Policy

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 4.01.

Technology 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 04.01: Technology Enablement Model

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

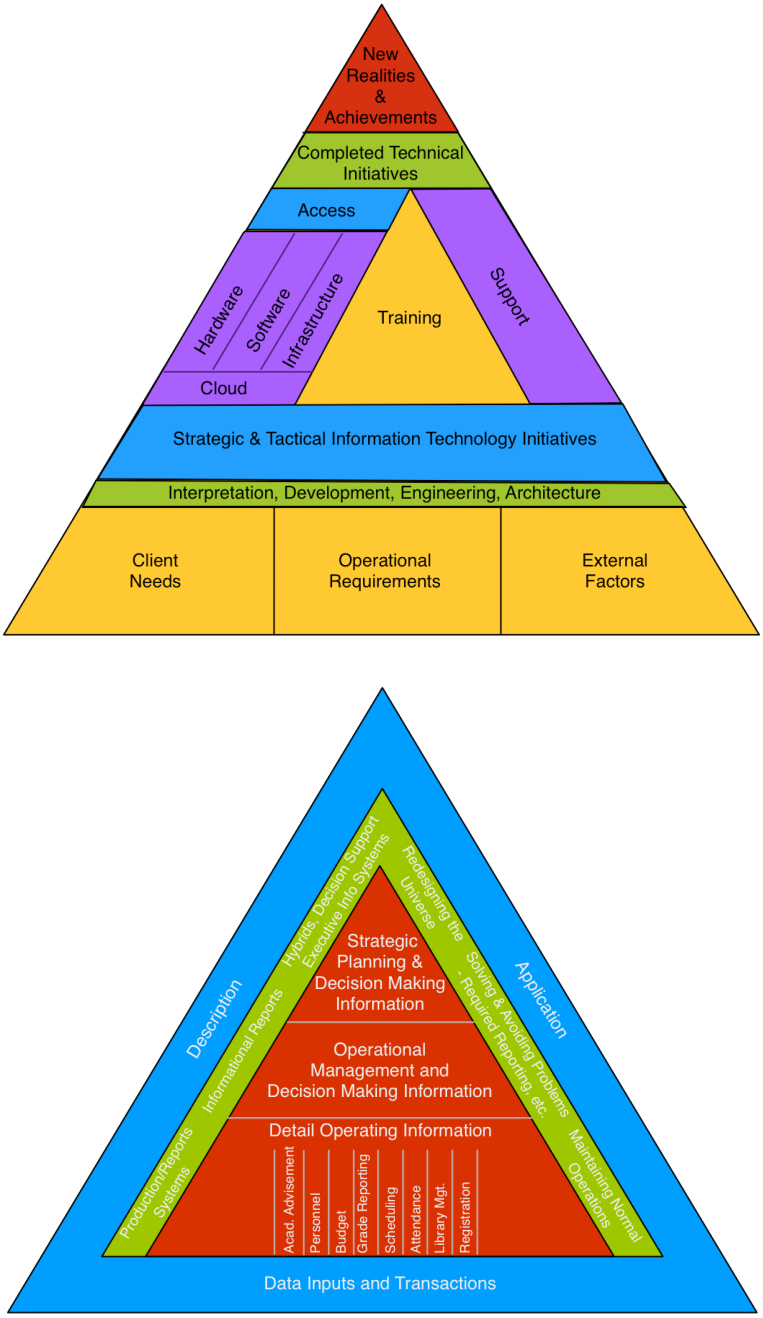


Figure 04.02: Information Levels and Functions Model

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.

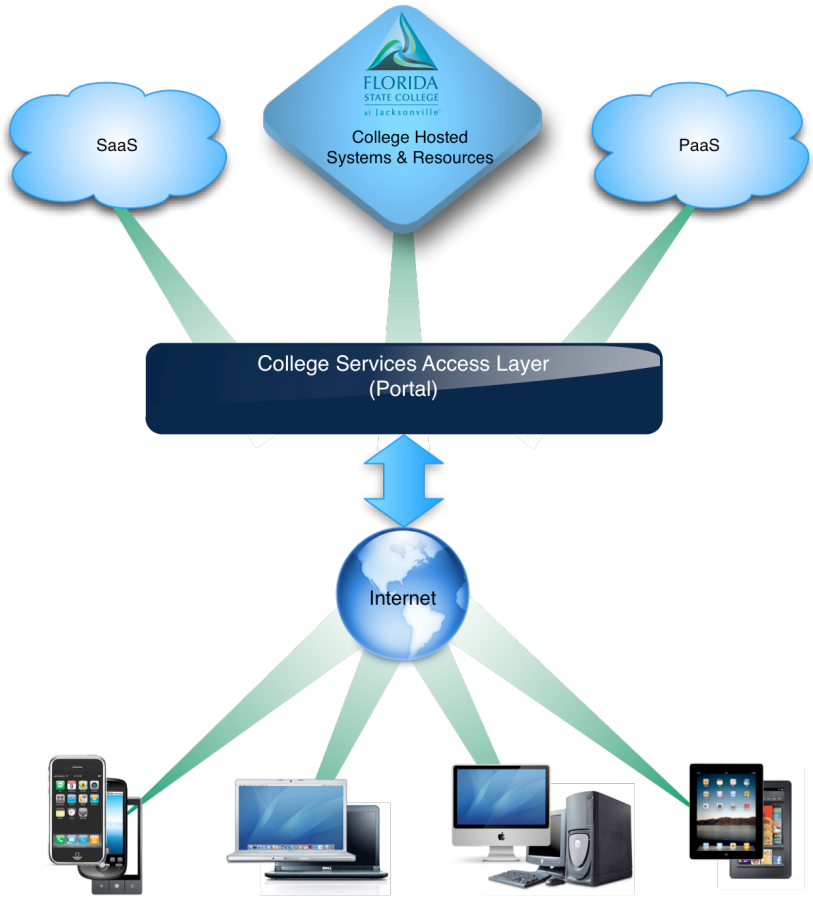


Figure 04.03: Technology Solutions Provisioning Model

04-03 • Hardware & Acquisitions [Smith]

Recommended and Reviewed By: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer

Management: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer

Purpose

The purpose of the policy is to provide information as it pertains to the standardization of college workstations, identify current standards for network servers on Florida State College production networks, identify and provide information as it pertains to the technological standardization of college classrooms and computer lab technology equipment, and to provide information as it pertains to standard and non-standard hardware acquisition college-wide. Reference policy and procedure *Technology Approval Due Diligence* in this section for description of the due diligence process of the technology division in the selection and approval of technology solutions.

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

Further detail regarding hardware is noted in the Technology Equipment Requirements documentation located in the Employee Portal in the Technology section.

Policy

Workstations

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

Servers

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 team, prior to ordering, shall approve server purchases. Technology Operations must also grant approval before moving servers into the production environment. New purchases of servers should be blade-type servers wherever possible.

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 and power supplies

- 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.

Regular 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

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 Team. 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 Executive Director of Technology Operations, Smart Classroom standards are evaluated in the fall of each year.

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.

Labs

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.

Hardware

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 Technology Department 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

Technology Department managers meet with the campus Directors of Administrative Services (DAS) and campus technology staff, to discuss and identify desktop and peripheral standards. The Technology Department in concert with the Academic Technology Committee define 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.

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.

Procedure

Workstations

Technology Department 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 five-year replacement cycle.

- Refer to the *Technology Equipment Requirements* in the Employee Portal under Technology
- 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 Microsoft System Center 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

Smart Classrooms

Newly acquired Smart Classrooms are to adhere to the *Technology Equipment Requirements*, construction should adhere to the *Technology Construction Requirements* (both of which are found in the Employee Portal) 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

Labs

- 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

Cell Phone Allowance

- The appropriate cabinet member brings the signed allowance request to Cabinet for consideration of employee cell phone allowance, 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

Non-standard Hardware

Any non-standard technology procurement requires consultation with and approval from the Director, Technology Administration. This will soon be located in the employee portal, Technology section within the IT Requests sub-section.

Non-standard Servers

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:

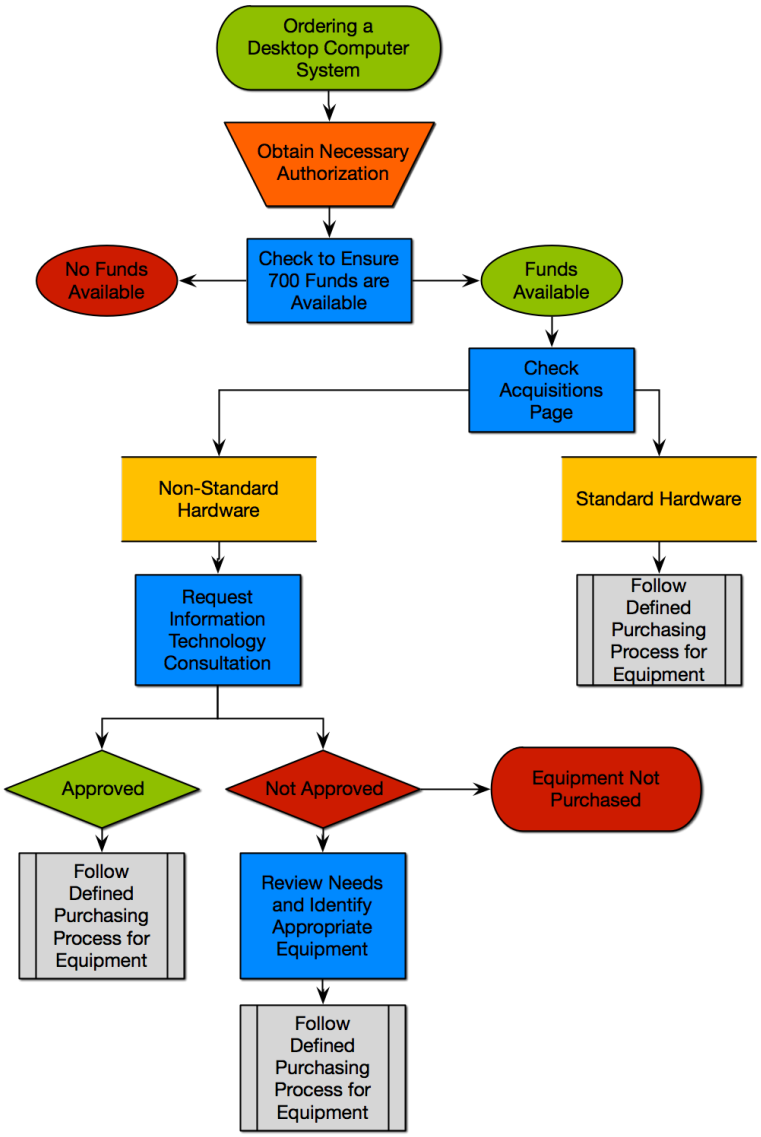


Figure 04.05: Purchasing Process

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

04-04 • Software Acquisitions [Thomas]

Recommended and Reviewed By: Kelly Thomas, Budget Analyst

Management: Kelly Thomas, Budget Analyst

Purpose

The purpose of this Technology Policy and Procedure is to provide information pertaining to the software acquisition process. Reference policy and procedure *Technology Approval Due Diligence* in this section for a description of the due diligence process of the technology division in the selection and approval of technology solutions.

Policy

Software acquisitions at Florida State College are designed to be a participatory process with the various constituencies of the college community and are conducted in adherence to Board of Trustees Rule 6Hx7--5.1. The Collegewide Academic Technology Committee, Center for Advancement of Teaching and Learning, campus faculty resource centers (FRC), and others contribute to what eventually defines the College's software acquisition process.

Procedure

This participatory acquisition process requires recommended software to overcome three separate, but intertwined procurement procedures.

1. The software must be endorsed by the specific campus/department and if it is academic software, there is a special form to complete and submit. This is located in the employee portal, Technology section within the IT Requests sub-section.
2. The software must pass the review and/or evaluation of the Technology Department.
3. The software must comply with the Purchasing Department's procurement procedures.

After meeting the requirements of these three procedures, the software can be acquired. In order to be placed on the list of approved software in Appendix A of the Strategic Technology Plan, the College President must also approve it.

Any software that passes the review and/or evaluation process of the Technology Department and is approved by the College President can be placed on the list in Appendix A of the Strategic Technology Plan. This permits for advance planning and expedited acquisition per Florida Regulations 6A-14.0734 – Procurement Requirements.

Further detail regarding software acquisition is noted in the Technology Software Acquisitions Requirements documentation located in the Employee Portal in the Technology section.

04-05 • Technology Approval Due Diligence [Smith]

Recommended By: Ron Smith - Executive Director of IT - CTO & CISO

Management: Ron Smith - Executive Director of IT - CTO & CISO

Purpose

The purpose of this policy and procedure is to describe the due diligence process of the Technology Department in the selection and approval of technology solutions.

Policy

The Technology Department is responsible for performing the 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. Technology solutions cover software, certain services, integrated solutions, cloud solutions, and hardware.

The following procedures are internal to the Technology Department and do not describe approval or due diligence procedures performed outside of the Technology Department.

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 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.

Procedure

Software

Beyond the four due diligence factors stated in the policy above, software is evaluated on purpose (academic or non-academic), status (already in the *Strategic Technology Plan*), location (server, desktop, etc.), distribution, and cost.

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. The Technology Department subjects integrated solutions to the applicable software and hardware acquisition procedures.

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

Reference *Technology Equipment Requirements* for information as it pertains to standards and requirements for hardware acquisition Collegewide. 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 documents and are reviewed quarterly and updated as necessary.

04-06 • Programming Standards [Martin]

Owner: Chris Martin, Executive Director of Information Systems
Management: Chris Martin, Executive Director of Information Systems

Purpose

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

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 Policy and Procedure *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.

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.

04-07 • DBMS Standards (admin) [Martin]

Recommended and Reviewed By: Chris Martin, Executive Director, Enterprise Applications

Management: Chris Martin, Executive Director, Enterprise Applications

Purpose

The purpose of this policy and procedure is to describe the the development and maintenance of databases supported by Data Management.

Policy

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

Procedure

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. Avoid storing calculated data in OLTP databases.
6. Either use full name or comprehensible abbreviation.
7. 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, Integration Services (SSIs) 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 must be performed by a DBA.
2. All database migrations must 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 should 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.

The DBA and or IT Team 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.

04-08 • Documentation [Martin]

Owner: Chris Martin, Executive Director of Information Systems

Management: Chris Martin, Executive Director of Information Systems

Purpose

This procedure provides the information for documenting the design, development, and implementation of web based applications by the E-Systems Team. These procedures may also apply to stand-alone applications.

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 (*Project Management Definition, Standards, and Financial Reporting* in section 10)
- Design Document/Storyboard (JIRA)
- Source Code in Repository [Source Safe/Team Foundation Server (2015 transition)]
- Testing (JIRA)
- Sign-off (JIRA)
- Change History (JIRA)
- Release History (Confluence)
- Application Downtime Report (Confluence)

All documentation shall be stored in accordance with policy and procedures *Library Management and Change Control* in section 07.

04-10 • Accessibility in Website and Application Development: [Martin]

Recommended and Reviewed By: Chris Martin, Executive Director of Information Systems

Management: Chris Martin, Executive Director of Information Systems

Purpose

The purpose of this policy and procedure is to identify the College's compliance with Section 508 of the Rehabilitation Act of 1973 as well as standards and regulations regarding the Americans with Disabilities Act (ADA) pertaining to accessible design for websites and applications developed by Florida State College at Jacksonville.

Policy

"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)

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. 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.

Web accessible sites and applications should provide an equal level of access regarding a variety of options, programs and hours of operation. A resource for web developers and designers is the Communications & IT section of the United States Access Board at www.access-board.gov .

The World Wide Web Consortium maintains a Web Accessibility Initiative guide to assist web developers with understanding best-practices on planning and implementing the inclusive sites at www.w3c.org/WAI."

Procedure

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

Resources & Contacts

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)

http://www.section508.gov/
http://www.access-board.gov/guidelines-and-standards
http://www.justice.gov/crt/508/report/content.php
http://www.w3.org/WAI/Resources/

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.

Operations

05-01 • ERP/ORION/PeopleSoft [Martin]

Recommended and Reviewed By: Chris Martin, Executive Director, Enterprise Applications

Management: Herman Möller, Director-IS, Applications

Purpose

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

Policy

Florida State College at Jacksonville utilizes an ERP system, known as Orion/PeopleSoft 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 is written in Natural, a 4GL programming language, with its associated database, ADABAS. PeopleSoft is a vendor developed application supported by Oracle. A staff of onsite and offsite programmer analysts database administrators, and systems programmers,support the system and environment.

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

05-02 • Production Scheduling [Martin]

Recommended and Reviewed By: Chris Martin, Executive Director, Enterprise Applications

Management: Rick Shierling, Information Technology Operations Manager

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 Operations to ensure that all production jobs are executed according to the daily production schedule.

Procedure

The daily production schedule is created, updated and maintained by Operations. In order to have a job executed:

- A formal request must be submitted to Operations in the form of an emailed parameter (parm) sheet.
- It is the responsibility of the requestor to specify all of the necessary parameter information
- Operations will not be held responsible for incorrect processing due to incorrect or missing parameter information

05-03 • Operating Environment and System Programming Services, Support Process, & ERP System Availability Schedule [Martin]

Recommended and Reviewed By: Chris Martin, Executive Director, Enterprise Applications

Management: Herman Möller, Director-IS, Applications

Purpose

The purpose of this section is to describe the College's enterprise system operating environment, programming services & support process and ERP system availability schedule.

Policy

ORION/PeopleSoft 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.

DAY	TIME
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 05.01: 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, 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 college-wide is located in the employee portal. This schedule is planned in advance and approved by the Florida State College Stakeholder Community.

Florida State College at Jacksonville performs its enterprise system (ORION/PeopleSoft) processing on an Oracle Enterprise Server. The server connects to SAN storage, as well as an Oracle backup system. The current Operating System (OS) is Sun Solaris.The maintenance and functionality of the OS is the responsibility of the Open Systems Team.

The Systems Programming/Application Support Team leader will manage the systems programming functionality including determining priorities and requirements.

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/Connections), comprise Florida State College's Enterprise Resource Planning (ERP) system.

Beyond the Solaris OS, 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.

05-04 • Batch Execution/UNIX Scripts [Martin]

Recommended and Reviewed By: Chris Martin, Executive Director, Enterprise Applications Management: Herman Möller, Director-IS, 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.

Procedure

The first steps in creating UNIX Scripts are:

- 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

Additional 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

05-05 • Documentation for Data Operations Center [Smith]

Recommended and Reviewed By: Ron Smith, Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer

Management: Ron Smith, Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer

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.

Policy

In order for data operators to execute jobs in the Data Operations Center, every process will be documented at the time of implementation. Such documentation will include the instructions, times at which jobs started and ended, and any relevant notes. All documentation will be filed in the Technology Operations area and kept readily accessible.

05-06 • Internet Domain Registration and Certificates [Smith]

Recommended by Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer
Management: Stephen Waddill, Systems Engineer

Purpose

The purpose of this policy is to provide standards to the purchase, maintenance, administration, and expiration of Internet domains and certificates.

Policy

All Internet domain and certificates are to be purchased through the Technology Department. 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.

Procedure

A Technology Department 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.

Databases & Database Management

05-08 • ADABAS References, etc. [Martin]

Recommended and Reviewed By: Chris Martin, Executive Director, Enterprise Applications

Management: 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.

Procedure

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

Additional resources from Software AG

- Release Notes
- Installation
- Adabas Documentations
- 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

05-09 • Solution Environment [Martin]

Recommended and Reviewed By: Chris Martin, Executive Director, Enterprise Applications

Management: 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.

Policy

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
EVENT REPLICATOR	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 05.02: Data Systems Solution Environment Products

Software Development Lifecycle (SDLC) & Change Management

07-03 • Natural Programming Guides [Martin]

Recommended and Reviewed By: Chris Martin, Executive Director, Enterprise Applications Management: Herman Moller, Director-IS, Applications

Purpose

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

Policy

- 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.gensystems.com/booklist_Natural.htm
- http://www.gensystems.com/booklist_NaturalConstruct.htm
- http://communities.softwareag.com/codesamples
- http://communities.softwareag.com/wiki/

07-04 • Methodology .Net/Java Architecture [Martin]

Recommended and Reviewed by: Chris Martin, Executive Director, Enterprise Applications

Management: Chris Martin, Executive Director, Enterprise Applications

Purpose

To identify and describe the disciplined programming methodology used by the E-Systems team to develop systems built with the .NET framework and Java Technology.

Policy

E-Systems Technology develops and supports advanced web applications that enhance the student's experience at Florida State College at Jacksonville. The dynamics of E-Systems projects require a disciplined approach that provides the environment for developing highly available products that quickly meet the clients needs and satisfactions.

Therefore, the E-Systems Team utilizes the eXtreme Programming (XP) methodology for the planning, designing, coding, and testing of web applications. In 2015, alternate agile development methodologies will be considered for the identification of a possible alternative to XP.

Procedure

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 Team 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.

Four 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

- 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
- 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/.

07-09 • Peer Review [Martin]

Recommended and Reviewed By: Chris Martin, Executive Director, Enterprise Applications

Management: 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.

Procedure

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

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

Programmer: Responsible for scheduling the code 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 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.

Information Security

Content Filtering

08-02 • Library Management [Martin]

Recommended and Reviewed By: Chris Martin, Executive Director, Enterprise Applications Management: Herman Möller, Director-IS, 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.

Policy

The Technology Department developed a system with restricted access to NATURAL libraries.

Procedure

The procedure is required to protect the NATURAL environment against unauthorized access and improper use.

If an employee needs access to a natural library, that individual shall:

1. Submit a request in writing to the Director of Information Systems (Applications).
    a. The request must specify the library involved.
    b. The reason access is needed.
    c. The time frame for which access is required.
2. After receiving the aforementioned information, the Director of Information Systems (Applications) shall grant or deny the request.
3. If the request is granted, the Director of Information Systems (Applications) will forward the original request to the Database Administrator (DBA).
4. The DBA will then process the request within the specified time frame.

08-03 • Florida State College at Jacksonville Content Filtering [Smith]

Recommended and Reviewed By: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer

Management: John Slevin, Director of Network Engineering

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.

Environmental

Logical Security

08-08 • External Data Extract Requests [Martin]

Recommended and Reviewed By: Chris Martin, Executive Director, Enterprise Applications

Management: Herman Möller, Director-IS, Applications

Purpose

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

Policy

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 and access to data will be restricted to ORION/PeopleSoft system areas allowed by the data owner. The requestor will be fully accountable for complying with Federal, State, and College policies in the management of college data.

Procedure

- A request must be submitted to 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 and a mutually accepted schedule will be adopted
- When required, personally identifiable information (as defined by the Florida Information Protection Act of 2014) shall be encrypted when at rest, in transit, and/or stored on portable storage devices (e.g. laptops, palm pilots, thumb drives, etc.)
- College personally identifiable information shall not be stored in personal cloud based storage (Dropbox, etc.)

08-09 • Florida State College Peer-to-Peer File Sharing [Smith]

Recommended and Reviewed By: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer Management: John Slevin, Director of Network Engineering

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.

Policy

Florida State College at Jacksonville utilizes a standalone Internet content filtering server appliance 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.

08-10 • Digital Signatures [Smith]

Recommended and Reviewed By: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer

Management: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer

Purpose

The purpose of this policy and procedure is to provide information regarding the use of digital signatures within Technology Department.

Policy

Applicable Federal and State laws govern the framework for the use and potential use of digital signatures at the College with 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.

Physical Security

08-12 • ERP Systems & Applications Security [Martin]

Recommended and Reviewed By: Chris Martin, Executive Director, Enterprise Applications

Management: Chris Martin, Executive Director, Enterprise Applications

Purpose

The purpose of this policy and procedure is to describe Enterprise Resource Planning (ERP) systems and applications security relating to the host operating system.

Policy

The main component of Florida State College's Enterprise Resource Planning (ERP) system, ORION/PeopleSoft 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 Systems Programming/Applications Support Team. ORION/PeopleSoft may be accessed 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/PeopleSoft, it does not provide access to modules. The second level of applications security is native within ORION/PeopleSoft 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/PeopleSoft 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.

Procedure

Access to ORION/PeopleSoft 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 Systems Programming/Applications Support Team upon request by Human Resources
- The Systems Programming/Applications Support Team and DBA, in conjunction with the Human Resources department, will monitor UNIX access to validate legitimate business needs for such access

08-13 • Data Security [Martin]

Recommended and Reviewed By: Chris Martin, Executive Director, Enterprise Applications

Management: Chris Martin, Executive Director, Enterprise Applications

Purpose

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

Policy

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, as defined by the Florida Information Protection Act of 2014 or legally protected means such as FERPA/HIPPA, etc., is intended for distribution within the College on a highly limited and restricted "need-to-know" basis only which, includes personally identifiable 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) - Utilizing highest bit size.

Reclassification of Information Resources

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

Procedure

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 and while in transit

- 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

Data Labeling

- All information assets or information processes, from the time of creation until they are destroyed, should be labeled (marked) using the information 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

Compliance & Regulatory Requirements and Reporting

Regulatory Requirements and Reporting

09-05 • Annual ERPM Reporting [Smith]

Recommended and Reviewed By: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer

Management: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer

Purpose

The purpose of this policy 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 Department requirement of this report and to ensure that the data submitted reflects, to the greatest extent practical, the technology at the College.

Project Management

10-01 • Project Management Definition, Standards [Martin]

Recommended and Reviewed By: Chris Martin, Executive Director of Information Systems

Management: Chris Martin, Executive Director of Information Systems

Purpose

The purpose of this section is to describe project management, the requirements and standards for project management, and to address financial management of technology projects under project management.

Policy

The Technology Department uses a flexible yet comprehensive rubric to manage technology projects. The Project Management Body of Knowledge (PMBOK) by the Project Management Institute (PMI - http://www.pmi.org) provides guidelines for defining, planning, and managing projects while the Technology Department ultimately decides exactly what qualifies as a project and what is required for proper management. A project is any task or set of tasks that represent a significant endeavor as determined by the Office of the CIO or its designee.

College technology projects are regularly approved and prioritized, but most commonly and rigorously during the Department's and College's annual budget preparations. Projects are envisioned, planned, coordinated, and managed by team leaders who provide financial estimates and break each project into conquerable tasks. Various project management tools and instruments are recommended and made available, particularly for task coordination, resource management, scheduling, and collaboration. Project prioritization is assessed and reassessed throughout the life of a project in order to balance and adjust for routine tasks, short term demands, critical interruptions, and especially the College's stated goals, priorities, and initiatives.

Procedure

- The Office of the CIO or its designee identifies a project
- Then the project is assigned a project code number - The project numbering schema is alphanumeric with the first character a letter 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
- Two types of project plans are recommended for use:
    1. The overview project plan that includes:
        - Project Number
        - Project Name
        - Project Synopsis
        - Project Personnel
        - Project Due Date & Milestones
        - Primary Tasks
        - Predecessors - Identified & Impact
        - Conflicts
        - Resource Requirements & Availability
        - Decision (financial) Packet
        - Comments

    The project registry and the overview project plans currently reside in the Confluence wiki under Technology Team Projects

    2. The detailed project plan is built from project planning software (e.g. Microsoft Project, OmniPlan) and includes as much or as little detail as determined necessary by the project lead or designee in order to accomplish the project
- Project plans should be reviewed and updated regularly to ensure accuracy and should include task addition, modification, and deletion as well as logistical adjustments for such things as internal or external delays
- All projects appear in the project registry and in one project classification; the project classifications are:
    - Requested
    - Active
    - Hold
    - Closed
- A project may move between classifications as its status changes
- Every expenditure by the Technology Department is recorded and is accompanied by a project code number which, permits for financial analysis and review of any project
- Three types of project closure are recommended:
    - A gap analysis from an outcomes instrument (form/survey) provided to the primary client/customer to complete for feedback

- A knowledge base review, update, and harvesting where critical information is collected from various project participants and added to the project code's wiki
- A financial analysis

10-02 • Service Request Process [Martin]

Recommended and Reviewed By: Chris Martin, Executive Director, Enterprise Applications Management: Herman Möller, Director-IS, Applications

Purpose

The purpose of this policy and procedure is to describe creation of the task list for each application area.

Policy

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

At the discretion of the Directors of Information Systems (Applications and E-Systems), issues may be forwarded to the Executive Committee for prioritization.

Procedure

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
- Specifying the following:
  - Components
  - Environment brief description
  - Type of issue
  - Reason for issue
  - Priority of issue
  - Time frame for which the issue is desired to be completed
  - Additionally, screen shots and wireframes can be attached to the request

10-03 • Process Measurement & Functional Evaluation [Martin]

Recommended and Reviewed By: Chris Martin, Executive Director of Information Technology

Purpose

The purpose of this policy and procedure is to provide information on the framework for process measurement and functional evaluation as used in the Technology Department.

Policy

The basis for process measurement and functional evaluation within the Technology Department is rooted in the organizational structure, driving philosophy; personnel, management, facilities, and operational processes used by the department to deliver 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 and ensure the execution of achievable plans. To do so, it will work with key stakeholders to ensure the a progress of its projects Process Management

The objectives of process management are to ensure that the processes within the department 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,. 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 Department are responsible for distribution, collection, and analysis of the outcomes survey.

10-04 • SCRUM [Martin]

Recommended and Reviewed By: Chris Martin, Executive Director, Enterprise Applications

Management: Chris Martin, Executive Director, Enterprise Applications

Purpose

The purpose of this 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.

Policy

Digital Media Productions 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 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 below, 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.

Procedure

The SCRUM method has three primary categories of implementation:

- Planning
  - Customer meeting and commitment
  - Storyboard and/or flowcharts depending on nature of project
  - Small milestones
  - Timelines
  - Customer agrees to plan and sign off on project upon completion
- Production
  - All aspects of production move forward simultaneously
  - Customer is involved during every step providing Q&A
  - Small milestones are achieved at a rapid pace
  - Small 15 minute one-on-one informal meetings are held to ensure daily progress

  - Full 1 hour team meetings are held every week to ensure everyone is working together
- Delivery
  - Since the customer has been providing Q&A throughout the project; this is a short step
  - Customer signs off on receipt of product

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

Third Party Service & Vendor Management

11-01 • Confidential College Information on Consultant/VendorEquipment [MARTIN]

Recommended and Reviewed By: Chris Martin, Executive Director, Enterprise Applications

Management: 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.

Policy

No sensitive data (personally identifiable data or confidential information) as defined by the Florida Information Protection Act of 2014 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.

11-02 • Service Level Agreements [Smith]

Recommended and Reviewed By: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer

Management: Ron Smith, Executive Director, Infrastructure, Operations, Service Management & CSO

Purpose

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.

Procedure

The Technology Department 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.

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

PRIORITY	ISSUE	CONTACT	RESOLUTION
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 11.01: Service Level Issues, Contact Timeline, and Resolutions

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.

11-03 • Systems Programming [Martin]

Recommended and Reviewed By: Chris Martin, Executive Director, Enterprise Applications

Management: Chris Martin, Executive Director, Enterprise Applications

Purpose

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

Policy

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.

11-04 • Technology Support Services [Martin]

Recommended and Reviewed By: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer Management: Ron Smith, Deputy Chief Technology Officer and Chief Information Security Officer Purpose

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

Procedure

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

1. For Faculty Support, dial 904-632-3151 then choose Option 1. This is for faculty members experiencing technical difficulties at a campus or center.
2. For password resets, Blackboard issues, or other technology issues dial 904-632-3151 then choose Option 3.

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. Contact information is found in the Employee Portal in the Technology section, Faculty and Staff Resources.

For Blackboard Training Classes:

Go to Employee Portal in the College section under the Quick Links area for the *AFPD Catalog* (*Academy for Professional Development*).

Technology Policies and Procedures

Florida State College at Jacksonville provides equal access to education, employment, programs, services and activities and does not discriminate on the basis of age, race, color, national origin, sex, disability, religious belief, or marital status. The College Equity Officer has been designated to handle inquiries regarding the non-discrimination policies and may be contacted at equityofficer@fscj.edu.

Florida State College at Jacksonville is a member of the Florida College System and is not affiliated with any other public or private university or college in Florida or elsewhere.

Florida State College at Jacksonville is accredited by the Southern Association of Colleges and Schools Commission on Colleges to award the baccalaureate and associate degree. Contact the Commission on Colleges at 1866 Southern Lane, Decatur, Georgia 30033-4097, or call (404) 679-4500 for questions about the accreditation of Florida State College at Jacksonville. The Commission is to be contacted only if there is evidence that appears to support an institution's significant non-compliance with a requirement or standard.