Gainesville State College

2012

System Security Plan

Office of Information Technology

Version 4.0

Confidential

Revision & Sign-off Sheet

Change Record

Date	Author	Version	Change Reference
2-15-2005	Alfred Barker	2.0	Revision of Document
9-22-2005	Alfred Barker	3.0	Revision of Document
12-18-2007	Alfred Barker	3.2	Complete End-of-Year Review
08-20-2008	Alfred Barker	4.0	Complete Revision
03-13-2009	Alfred Barker	4.0	Review – minor edit corrections
12-05-2009	Alfred Barker	4.0	Add DPM changes Fault Tolerance
03-31-2011	Alfred Barker	4.0	Added Secure Portal information throughout document and removed Fault-Tolerance to create its own plan.

Reviewers

Name	Version Approved	Position	Date
Rick Coker	Version 1.0	Chief Information Officer	12-13-2004
Brandon Haag	Version 1.0	Asst. Dir.	12-13-2004
Rick Coker	Version 2.0	Chief Information Officer	2-15-2005
Brandon Haag	Version 2.0	Asst. Dir.	2-15-2005
Brandon Haag	Version 3.0	Chief Information Officer	12-18-2007
Brandon Haag	Version 4.0	Exec. Dir.	03-13-2009

Distribution

Name	Location
Backup Copy	Dunlap Mathis Building, Rm. 132
Original Copy	ACAD III, Rm. 175
Electronic Copy	https://portal.gsc.edu/depts/it/default.aspx?page=View=Shared

Document Properties

Item	Details
Document Title	System Security Plan
Author	Alfred Barker
Document Manager	Alfred Barker
Creation Date	12-13-2004
Last Updated	04-04-2012

This page is intentionally left blank

TABLE OF CONTENTS

Figures amd Tables

Executive Summary

Security architecture is a set of plans and principles that describes how to best implement the security controls and services a system should provide to deal with the system's threat environment. More thorough security architecture must deal with both intentional, intelligent threats and accidental kinds of threats, which often includes a firewall to protect against Internet threats as well the basics of computer, personnel, physical, and procedural security, such as classifying and labeling data and services according to sensitivity, protecting access to workstations, running anti-virus software, and tracking removable media.

The first step in designing an organization's security architecture is to identify the organization's assets. Once identified, enumerate the potential threats to those assets and then create the security policies and procedures needed to address them. These security policies and procedures reflect the attitude that Gainesville State College will take toward securing its resources. This includes the value placed on resources held by the College and what it deems to be an acceptable risk for the protection of those resources. The *System Security Plan* and its associated policies, plans, and procedures will define the college's security expectations. As with all policies, plans, and procedures, once developed, an organization can use it as a guideline for developing future security plans. Included in this section are statements of:

- Purpose
  - System Security Plan
  - Strategic Plan
  - Securing the Logical Infrastructure Plan
  - Securing the Physical Infrastructure Plan
  - Plan, Policies, Procedures, Standards, and Configuration Guides
- Authority
- Compliance
- Continuance

Purpose

This *System Security Plan* defines the security needs of Gainesville State College by identifying the following:

- **Resources to be protected.** Several resources in an organization may require protection, including hardware, software, and data. In some situations resources may include the people who know the security designs implemented for an organization. *(Reference: III. Protection of Critical Institutional Computing Resources – Classifying Assets and Incident Response Plan.)*
- **Threats Faced by the Resources.** By identifying the threats that the college's resources face, Office of Information Technology can assign a value to the potential loss if the resource is compromised. Typical threats include unauthorized access to a resource and denial of service where the resource can't be accessed. *(Also reference: I. Institutional Profile – Risk Management – The Tolerance of Risk and Incident Response Plan.)*
- **Probability of the Threat Occurring.** Before developing a security plan to minimize the effect of a specific threat, the Information Technology staff must constantly evaluate likely threats. *(Also reference: I. Institutional Profile – Risk Management – The Tolerance of Risk and Incident Response Plan.)*

By identifying the resources, the threats, and the probabilities of the threats, Gainesville State College's Office of Information Technology shall be better able to design security architecture of policies and procedures that address the ever changing world of threats and recommend a course of action to take if and when the threats occur.

The Office of Information Security – USG has mandated the need to annually report the status of GSC's *Information Security Program Report*. This report is focused on six goals. *The System Security Plan (SSP)* has placed the goals along with the relevant information and strategies, initiatives and question pertinent to each goal.

System Security Plan

The *System Security Plan* consists of four sections designed to map to the *Board of Regents' Institutional Security Plan and Reporting Minimums – Recommended by the Security Advisory Group and ACIT Volunteers, Fall 2006.* On overview of the sections are as follows:

Executive Summary – this section addresses the purpose, authority, compliance, and continuance of the *System Security Plan*, while also addressing Risk Assessment and Review, Policy Creation, Procedures to Implement Policy, and Auditing.

I. Intuitional Profile – this section addresses Institutional Structures; Determining College, Technical and Security Requirements; accountability of Assets; Outsourcing; Learning from Incidents and the Privacy Impact Statement.

II. Institution-wide Policies and Security Procedures – this section covers the Acceptable Use Policy; Electronic Mail Security; Managing Passwords; Personnel Security – User Rights and Responsibilities; Training Opportunities and Reporting and Handling Security Incidents.

III. Protection of Critical Institutional Computing Resources – this section addresses Classifying Assets; Secure Handling, Storage and Disposal of Information and Media; Physical Security – Securing the Physical Infrastructure; Securing Power Supplies; Controlling Access to Networks and Systems, Protecting Against Malicious Software; Implementing Encryption Techniques; and Developing Back-up Procedures – Fault Tolerance Measures.

Strategic Plan

Goal 1: Institution's security goal(s), strategy, initiatives w/plan-of-action and milestones.	**Possible Strategies /Initiatives/Questions:**
The Strategic Plan consists of a formal document addressing the Office of Information Technology's: Mission Statement, Vision Statement, Shared Values Statement, and Strategic Goals, which map to the strategic goals of Gainesville State College (GSC). These goals are as follows: 1. *Provide outstanding operation, development, reporting and integration services for academic and administrative systems, whether local, centrally hosted or outsourced.* 2. *Operate and maintain a seamless and reliable network, server, voice and video communications infrastructure across multiple campuses.* 3. *Install, maintain and upgrade faculty, staff and student computers, peripherals and software in order to satisfy new requirements and maintain technical currency.* 4. *Continue to improve campus IT security, work on the comprehensive IT security plan and provide IT security information and training for faculty, staff and students.* 5. *Provide world-class customer support and services by attracting, training, equipping and retaining a skilled IT workforce.*	A more thorough exploration of this topic is located in the Strategic Plan. The Strategic Plan is GSC's IT Five-Year planning tool. The above listed documents may be provided upon request. The responsibility for coordinating and implementing any projects listed is the Information Security officer at GSC.

Securing the Physical Infrastructure Plan

This document discusses topics such as: institutional structures, determining technical and security requirements – i.e., information sensitivity and criticality, application and systems categorizations, risk assessment, accountability of assets, outsourcing, after action reviews, and privacy impact statements.

- *https://portal.gsc.edu/depts/it/default.aspx*

Securing the Logical Infrastructure Plan

This document covers filters and firewalls, protocols and standards, VLANS, SNMP, WINS, certifications and encryption, remote access, and software usage. Also included is the enterprise services security: domain controllers, DNS, DHCP, Exchange, IIS and SQL. Fianally auxciliary service security is addressed to include: VoIP, VMWare, and open source systems.

- *https://portal.gsc.edu/depts/it/default.aspx*

While it seems that Gainesville State College would assign maximum security to all their resources, costs often limit security implementations. These costs aren't only financial costs, but also performance and ease-of-use costs.

Generally, security policies, procedures, and plans are designed based on trade-offs between:

- **Functionality versus Security.** Sometimes organizations require the use of a service on the network. The service provides some form of functionality to the organizations even though the service introduces security risks, for example, wireless access. *(Also reference: Securing the Wireless Network Plan).* In this case the security plan costs must not outweigh the benefit received by the service's added functionality.
- **User Convenience versus Security.** The policy and/or procedure must identify when security becomes a barrier to users performing their jobs, such as Faculty and Staff.
- **Cost and Functionality.** The policy and/or procedure must propose security plans that fall into the College's budget. If the security level required by the policy and/or procedure isn't affordable, the policy and/or procedure cannot be followed and must be revised.

Plans, Policies, Procedures, Standards and Configuration Guides

RFC 2196 Sec.3.1.1 states the Security Architecture, "should be crafted as a framework of broad guidelines into which specific policies will fit." The policies, procedures, and plans currently in use or under development are utilized by Gainesville State College for the purpose of securing the computer and network assets. The comprehensive security documentation is listed on the secure IT portal:

- *https://portal.gsc.edu/depts/it/default.aspx*
- **Plans:**
  - *Backup and Fault-Tolerance Plan*
  - *Communications Plan*

    The *Communications Plan* will document the contact lists, roles, and methods of contacting members of the Office of Information Technology.
  - *Disaster Recovery Plan*

    The *Disaster Recovery Plan*'s primary focus is to provide a programmed response to a disaster that destroys or severely cripples the College's central computing and networking systems operated by the Office of Information Technology. The secondary focus is to describe a number of measures taken to mitigate or minimize the effects of a potential disaster.
  - *HEOA Compliance Plan*
  - *Incident Response Plan*

    The *Incident Response Plan* details the steps taken to respond to incidents and follow-up afterwards. This document focuses on security threats and risk assessments, breach and hacking prevention, and the processes of response.
  - *Information Security Awareness and Training Plan*

- *IT Business Continuity Plan*
- *Log Management Plan (Under Development)*

  The *Log Management Plan* will describe the logging controls to be put into place to provide early warning as well as forensic capabilities to meet potentially future logging requirements.
- *PCI Compliance Plan*
- *Securing the Logical Infrastructure Plan*

  The *Securing the Logical Infrastructure Plan* is the flag-ship document designed to secure Gainesville State College's system, network, and auxiliary services through the use of best practices and checklists.
- *Securing the Physical Infrastructure Plan*
- *Securing the Wireless Network Plan*
- *Strategic Plan*

  The *Strategic Plan* is a five-year look at the mission, vision, shared values and goals of the Office of Information Technology.
- *System Security Plan*

  The *System Security Plan* is cornerstone document form which all Gainesville State College's Information Technology systems security-based plans, policies, procedures, standards, and configuration guide support. This is a system wide document designed to address the processes and procedures for securing the College's computing and networking systems and environment.

- **Policies:**
  - *Allocation of IT Resources Policy*
  - *Audit and Vulnerability Scan Policy*

    The *Audit and Vulnerability Scan Policy* establishes the responsibility of the Office of Information Technology to conduct audits and vulnerability scans and the authority to conduct such activity, while understanding that such scans may have potential costs.
  - *Change Control and Problem Management Policy (Under Development)*

    The *Change Control and Problem Management Policy* describes the methodology employed by Gainesville State College in the support of Change Control and Problem Management for both the Academic and Administrative Computing.
  - *Computer and Network Usage Policy (a.k.a Acceptable Use Policy)*

    The *Computer and Network Usage Policy* is a college-wide policy intended to allow for the proper use of all Gainesville State College computing and networking resources, effective protection of individual users, equitable access, and proper management of those resources.
  - *Document Classification Policy*

    The *Document Classification Policy* outlines the definition and assignment of document/data classification of the plans, policies, and procedures of the Information Technology resources of Gainesville State College.
  - *Electronic Equipment and Media Disposal Policy*

    The *Electronic Equipment and Media Disposal Policy* outlines the materials and the methodology currently used by the College Information Technology staff to properly dispose

of electronic equipment and various forms of media. This policy acts as an extension of the *System Security Plan*.

- *Enterprise Firewall Policy*

  The purpose of the *Firewall Policy* is to establish the what, where, who and why for implementing, managing, and maintaining the appliance and its associated policy.

- *Enterprise PacketShaper Policy*

  The purpose of the *PacketShaper Policy* is to establish the what, where, who and why for implementing, managing, and maintaining the appliance and its associated policy.

- *Enterprise Wireless Access Control Policy (Under Development)*

  The *Wireless Access Policy* outlines wireless security issues, best practices, deployment standards, user conduct and network guidelines, and the locations of the College access zones.

- *Information Security Awareness and Training Policy (Under Development)*

  The *Training Policy*'s purpose is one of educating the campus population to the acceptable use of the computing and networking resources.

- *Mobile Storage and Computing Device Policy*

  The purpose of the Mobile Storage and Computing Device Security Policy is to establish safeguards for the use of mobile media and computing devices, including their connection to the Gainesville State College network.

- *Official Gainesville State College E-Mail Policy*

  The *Official Gainesville State College E-Mail Policy* recognizes the use of the College assigned e-mail account as a mechanism for official communication within the College.

- *PeopleSoft User Security Policy*

  The *PeopleSoft User Security Policy* is designed to ensure that users within the PeopleSoft Human Resources and Accounting and Finance system have the security context approved by the owner of the respective system

- *Servicing and Supporting Personal Equipment Policy*

  The *Servicing and Supporting Personal Equipment Policy* defines that no service or support of personal computing equipment will be permitted except that service that is under an independent contractual agreement.

- *Software Usage Policy*

  The *Software Usage Policy*'s objective is to supply Gainesville State College users with the most reliable computer systems possible, which includes ensuring the use of the latest software and the newest technology available and take every action to protect the integrity and privacy of the users' data.

- *Systems Security Policy*

  The *Systems Security Policy* outlines the methodology adopted by the Information Technology staff to secure the resources of Gainesville State College.

- *Telecommunications Policy*

  The *Telecommunications Policy* for Wireless Devices / Cellular Telephones and Long Distance Usage was developed to define the purpose behind the policy's implementation, to give general guidelines for acquisition and use, and to establish criteria for determining need. Also covered within this policy is the description of personal usage of and the administrative processes for ordering and making payments on College owned telecommunication devices.

Finally, this policy discusses what is and is not permitted in regards to long distance telephone usage.

- Users Password Credentials Policy

  The *Users Password Credentials Policy* is designed to secure Gainesville State College computer and network resources by outlining the handling, composition, password change procedures, support, and responsibilities of password credentials.

- Video Surveillance Policy

  The *Video Surveillance Policy* outlines and defines the processes, standards, and responsibilities of requesting, planning, implementing and maintaining a video surveillance infrastructure. In addition, this policy defines "unauthorized use" of the surveillance equipment.

- **Procedures:**
  - Administrative Procedures for User Accounts in Academic Computing

    The *Administrative Procedures for User Accounts in Academic Computing* provides the administrator with a step-by-step guide for the creation and removal of Faculty and Staff accounts for the academic computing environment.

  - Camera Procedures Guide

    The *Camera Procedures Guide* outlines the College's adoption of *Axis Communications* and defines the processes, standards, and responsibilities of requesting, planning, implementing and maintaining a video surveillance infrastructure.

  - DMCA/RIAA Notification Reporting Guide

  - Hardening ProCurve Security Procedures

    The purpose of this procedure is to outline provisions for protecting access to the switch's status information and configuration settings. ProCurve switches are designed as "plug and play" devices, allowing quick and easy installation in the network.

  - Procedures for Change and Configuration Management *(Under Development)*

    The *Procedures for Change and Configuration Management (Under Development)* discusses the main processes and activities involved in change and configuration management. This guide is closely modeled off of the Microsoft Operation Framework Process Model.

- **Standards:**
  - Cabling Plant Standard

    The *Cabling Plant Standard* describes the details needed when installing or upgrading the copper and/or fiber data and voice cabling infrastructure. A key use of the standard is in the bidding process to establish the quality and type of work expected.

  - Video Surveillance Standards

    The Video Surveillance Standard outlines the College's adoption of a video surveillance system, standards of enterprise cabling and unique identification of its cabling infrastructure.

- **Configuration Guides:**
  - DMCA/RIAA Reporting Guide

- The *DMCA/RIAA Reporting Guide* outlines the methodology currently used by the College's Information Technology staff to receive, verify and resolve the notification of violation from the DMCA or RIAA.
- Environmental Monitor Configuration Guide *(Under Development)*

  This guide to be written in the near future – technology is deployed.
- "EZProxy" Proxy Configuration Guide

  The "*EZProxy"Configuration Guide* provides notes and screenshots of the configuration of the EZProxy Server known as RESOURCE.
- GSC Videoconferencing Configuration Guide

  The *GSC Videoconferencing Configuration Guide* is yet another compilation of screen shots used to record the configuration settings for three different Tandberg systems.
- Terminal Services and HVAC Configuration Guide

  The ALCSERVER and SACSERVER are the central communication and control mechanism in support of the ACL's and Siemens centralized HVAC management process. These servers host a web-based controller interface, which allows the HVAC controlling units to be managed centrally via the servers. The technology utilized to make remote management possible is Windows Server 2003 with Terminal Services.
- Watchdog Environmental Monitor Configuration Guide

  The *Watchdog Environmental Monitor Configuration Guide* captures in screen shots the configuration setting used to keep the environmental monitor properly functioning.
- Wireless Access Management Configuration Guide

  The *Wireless Access Management Configuration Guide* describes the configuration of the wireless access points and their association with the Access Control Server, and the configuration of the ACS and the centralized nature of management of the wireless network. This document's main purpose is as a disaster recovery tool.

Authority

Section 712 of the Policy Manual of the Board of Regents in part states,

> "The University System Office and all System institutions have the responsibility to employ prudent information security policies, standards, and practices to minimize the risk to the integrity, confidentiality, and availability of University System information.
>
> Therefore, the University System Office and all System institutions shall create and maintain an internal information security technology infrastructure consisting of an information security organization and program that ensures the confidentiality, availability, and integrity of all University System information assets.
>
> USG-OIS will be compiling the USG institutions' information security program status reports into a single report, which is to be available by October 31st of each year."

Gainesville State College's Executive Committee fully supports the *System Security Plan* and all of the associated plans, policies, and procedures. The Office of Information Technology manages and administers the *System Security Plan* and all associated plans, policies, and procedures, which is currently in effect for all of Gainesville State College, students, employees, and computer systems.

Compliance

This document is consistent with the *Board of Regent's Policy Manual, Section 712.03* and the broad guidelines provided by the Security Advisory Group's documentation and audit reviews.

Also considered, the Board of Regents of the University System of Georgia's *Business Procedures Manual, Section 12.0 Protection and Security of Records.*

The standard on which this document has been established is based on the *Institutional Security Plan and Reporting Minimums – recommended by the Security Advisory Group and ACIT Volunteers, Fall 2006.*

Continuance

This *System Security Plan* and its associated plans, policies, and procedures are a living document and may be modified at any time by the Office of Information Technology or the executive committee. *Figure A* depicts the policy and procedure life cycle.

Goal 2: Develop, Approve, and Promote a Comprehensive Information Security Policies and Standards Suite. Include strategy, initiatives w/plan-of-action and milestones.	**Possible Strategies /Initiatives/Questions:**
GSC has not adopted any third-party InfoSec policy "development model." However, GSC has created a development standard based on and adopted from a compilation of best-practices. This consistent, documented, and repeatable process consists of: **Risk Assessment and Review** Risk assessment, as defined and understood by the Office of Information Technology, is the process by which risks are identified and the impacts of the risks are determined. The methodology adopted by the College for risk analysis and subsequent management was influenced by Microsoft's *Security Risk Management Guide*. To ascertain a deeper understanding of the assessment process, reference: *Institutional Profile* of the *System Security Plan*. The primary responsibility of the currency and accurately of this document is the Office of Information Technology. The *Document Properties* section of the *Revision & Sign-off Sheet* located on Page 3 lists the person or personnel that have been assigned the specific responsibility of this document. Also listed is the *Change Record* table where *Date*, *Author*, *Version*, and *Change Reference* can be recorded. If the original assessment were affected by any change, a process of review would take place in response. Examples of change are: identification of new vulnerabilities, significant security incidents, and changes to organizational and technical infrastructure. Also listed on the *Revision & Sign-off Sheet* is the *Reviewers* table where personnel can record they have reviewed the policy changes, and the *Distribution* table where the document's location and person or personnel responsible can be recorded.	• A more thorough exploration of this topic is located in the *System Security Plan –Executive Summary*. • No 3rd party management framework has officially been adopted. Many plans, policies, and procedures guides are "Best Practices" based – examples are: HP, Microsoft, SANs, and ISO 27000 series. • GSC's *System Security Plan* framework is based on the ACIT SAG's "Institutional Security Plan & Report Minimums." • GSC is exploring CobiT 4.x as a possible framework for future use – but is reserving adoption until BOR's ISO makes a determination on the direction he wants to move. ▪ The above listed documents may be provided upon request. ▪ The responsibility for coordinating and implementing any projects

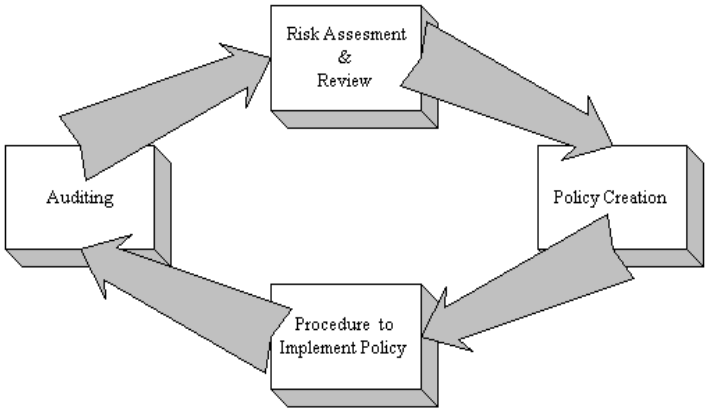

Figure: Policy and Procedure Life Cycle

Policy Creation

Every plan, policy, and procedure begins as a fact-finding, data-gathering process, which is formalized into a draft document by the Document Manager. The document is reviewed by the appropriate system owners and the Information technology staff for accuracy. This process continues until the document is complete. The document is then classified *(Reference: Document Classification Policy)* and prepared in its final format for submission.

Procedure to Implement Policy

The Chief Information Officer of the Office of Information Technology presents the final formatted document for review to the President and the Executive Council. If approved, the document receives the authority necessary to be enforced and is published in accordance with its classification. If unapproved, the document returns to the Policy Creation phase and is re-evaluated and re-submitted after the requested or required changes have been included or excluded. Awareness of the policy is based on its classification.

Auditing

Auditing is an ongoing process, whereas the *Audit and Vulnerability Policy* establishes responsibility and authority, the *System Security Plan* describes the processes used to conduct audits. The *Detailed Institutional System Security Plan (SSP) Review* below is a self-audit form-based process utilized by the Office of Information Technology to assist in the auditing of the plans, policies, and procedures.

Detailed Institutional System Security Plan (SSP) Review

The Office of Information Technology at Gainesville State College has adopted a self-audit position to insure that the *System Security Plan*, and its associated plans, policies and procedures remain current and are in accordance with the broad guidelines provided by the Security Advisory Group in the form of the *Enterprise Infrastructure Services, ITS Security, Gainesville State College Campus Security Plan, Detailed Review*.

listed is the Information Security officer at GSC.

- AUCPA has not been evaluated – what we have seems appropriate.
- The *Securing the Physical and Logical Infrastructure Plans* are mature documents that were once part of a single document, but have been removed to create stand alone documents.
- The *Communications Plan* too is now to be a standalone document, which was once part of the *Disaster Recovery Plan*.

Table A: lists the evaluation minimums and the security documentation reference locations. Note (SSP) denotes *System Security Plan*:

Evaluation Categories	Reference Location(s)
A. Application/System Identification	
A.1 Application/System Category	• Institutional Profile (SSP) o *Determining Security Requirements* ▪ Application / System Category
A.2 Application/System Name/Title	• Institutional Profile (SSP)
A.3 Responsible Organization	• Institutional Profile (SSP) o *Institutional Structures* • Disaster Recovery Plan • Incident Response Plan
A.4 Information Contact(s)	• Institutional Profile (SSP) o *Institutional Structures* • Disaster Recovery Plan • Incident Response Plan
A.5 Assignment of Security Responsibility	• Institutional Profile (SSP) o *Institutional Structures* • Disaster Recovery Plan • Incident Response Plan
A.6 Application/System Operational Status	• Institutional Profile (SSP) o *Application / System Operational Status*
A.7 General Description/Purpose	• Executive Summary (SSP)
A.8 Application/System Environment	• Institutional Profile (SSP) o *The Tolerance of Risk* o *Threat Analysis Results* o *Threat Matrix* o *Defense Methodology*
A.9 Application/System Interconnection/Information Sharing	• Securing the Physical Infrastructure Plan o *Physical Fiber Plant Diagrams* • Securing the Logical Infrastructure Plan o *Diagrams of the Logical Network / Data Flow* o *Securing Remote Access* • Securing Windows 2003 Domain Controllers and Active Directory (SSP) o *Sites*
A.10 Applicable Laws or Regulations Affecting the Application/System	• Institutional Profile (SSP) o *Determining Gainesville States College's Requirements* ▪ Federal Laws ▪ State Laws
A.11 Information Sensitivity and Criticality Assessment	• Institutional Profile (SSP) o *Deterring Security Requirements* o *Information Sensitivity and Criticality Assessment* o *Appendix B*
A.12 Privacy Impact Assessment	• Institutional Profile (SSP) o *Privacy Impact Statement*
B. Management Controls	
B.1 Risk Assessment and Management	• Institutional Profile (SSP) o *Determining Security Requirements* o *The Tolerance of Risk* o *(A more formal procedure guide is under development)*

B.2 Review of Security Controls	• Executive Summary (SSP)
	  o *Review & Evaluation*
	• Institutional Profile (SSP)
	  o *Reporting and Handling Security Incidents*
	• **Note:** Every Plan, Policy, and Procedures document has a "Revision & Sign-off Sheet" to record changes.

B.3 Rules of Behavior - Institutional Acceptable Use Policy	• Executive Summary (SSP) o *Authority, Continuance, and Compliance…* • **Note**: Every Plan, Policy and Procedure document has statements of "Authority," "Continuance," and "Compliance."
B.4 Planning for Security in the Life Cycle	• Executive Summary (SSP) o *Continuance* • **Note**: Every Plan, Policy and Procedure document has a "Continuance" statement.
B.5 Certification and Accreditation	• **Note**: Every Plan, Policy and Procedure document has an "Authority" statement, no additional letters or certificates are currently required.
C. Operational Controls	
C.1 Personnel Security	• II. Institution-wide Policies and Security Procedures – Personnel Security – User Rights and Responsibilities (SSP) • PeopleSoft User Security Policy • Users Password Credentials Policy
C. 2 Physical and Environmental Protection	• Securing the Physical Infrastructure Plan • Disaster Recovery Plan • Computer and Network Usage Policy

C.3 Production, Input/Output Controls	• Securing the Physical Infrastructure Plan
	  o *Secure Disposal of Equipment*
	• Securing Windows 2003 Domain Controllers and Active Directory (SSP)
	  o *Security Template Audit*
	  o *Active Directory Auditing*
	  ▪ Recommended Audit Policy

C.4 Contingency Planning and Disaster Recovery	• III. Protection of Critical Institutional Computing Resources – Protecting Against Malicious (SSP) • III. Protection of Critical Institutional Computing Resources – Developing Back-up Procedures (SSP) • Change Control and Problem Management Policy • Disaster Recovery Plan • Procedures for Change and Configuration Management • Configuration Guides

C.5 Application/System Configuration Management Controls	• Executive Summary (SSP)
	  o *Configuration Guides*
	  o *Review & Evaluation*
	• Institutional Profile (SSP)
	  o *Learning from Incidents*
	• Securing Windows 2003 Domain Controllers and Active Directory (SSP)
	  o *Active Directory Change Plan*
	• III. Protection of Critical Institutional Computing Resources – Developing Back-up Procedures (SSP)
	  o *Notification and Restoration*
	• III. Protection of Critical Institutional Computing Resources – Developing Back-up Procedures (SSP)
	• III. Protection of Critical Institutional Computing Resources – Protecting Against Malicious (SSP)

C.6 Data Integrity/Validation Controls	• Fault Tolerance Measures (SSP)

	○ *Preparation / Data Maintenance* • Change Control and Problem Management Policy
C.7 Documentation	• Executive Summary (SSP) ○ *Purpose* ○ *Review & Evaluation* • Document Classification Policy • **Note:** Every Plan, Policy, and Procedures document has a "Revision & Sign-off Sheet" to record changes.
C.8 Security Awareness Training	• II. Institution-wide Policies and Security Procedures – Personnel Security – User Rights and Responsibilities (SSP) ○ *Training Opportunities* • Training Policy
C.9 Incident Response Capability	• Disaster Recovery Plan • Incident Response Plan • **Note:** mitigation through the implementation of the System Security Plan.
D. Technical Controls	
D.1 Identification and Authentication	• II. Institution-wide Policies and Security Procedures – Personnel Security – User Rights and Responsibilities (SSP) ○ *Access Control* • Securing Windows Domain Controllers and Active Directory (SECURING THE LOGICAL INFRASTRUCTURE PLAN) ○ *Domain Account Policy* ○ *Active Directory Auditing* ○ *Active Directory Based Secure Communications* • Computer and Network Usage Policy • PeopleSoft User Security Policy • Users Password Credentials Policy • Administrative Procedures for User Accounts in Academic Computing
D.2 Logical Access Controls	• Securing Windows Domain Controllers and Active Directory (SECURING THE LOGICAL INFRASTRUCTURE PLAN) ○ *Organizational Units* ○ *Active Directory Audit* ○ *Kerberos Policy* ○ *Security Templates* ○ *Active Directory Policy Based Secure Communications* • Securing the Logical Infrastructure Plan ○ *Perimeter Layer Security* ○ *Network Layer Security* ○ *Securing Remote Access* • Securing Internet Information Service (SECURING THE LOGICAL INFRASTRUCTURE PLAN) ○ *Securing IIS - Authentication*
D.3 Public Access Controls	• Securing the Logical Infrastructure Plan ○ Certificates, Encryption, and Virtual Private Networks • Securing Windows Domain Controllers and Active Directory (SECURING THE LOGICAL INFRASTRUCTURE PLAN) ○ *Domain Account Policy* • Securing Internet Information Service (SECURING THE LOGICAL INFRASTRUCTURE PLAN) ○ *Securing IIS - Authentication* • Securing Wireless Access (SECURING THE LOGICAL INFRASTRUCTURE PLAN) • Computer and Network Usage Policy • Official Gainesville State College E-Mail Policy • PeopleSoft User Security Policy

	• Users Password Credentials Policy
D.4 Audit Trails	• Securing Windows Domain Controllers and Active Directory (SECURING THE LOGICAL INFRASTRUCTURE PLAN) o *Active Directory Auditing* • III. Protection of Critical Institutional Computing Resources – Developing Back-up Procedures (SSP) o *The Auditing Process – Phase II* • III. Protection of Critical Institutional Computing Resources – Developing Back-up Procedures (SSP) o Assessment and Auditing Procedures • Change Control and Problem Management Policy • Procedures for Change and Configuration Management • Configuration Guidelines • Incident Response Plan

Table: Security Plan – Evaluation Minimums