Gainesville State College

2012

Securing the Physical Infrastructure Plan

Office of Information Technology

Version 1.0

Sensitive

Revision & Sign-off Sheet

Change Record

Date	Author	Version	Change Reference
03-12-2009	Alfred Barker	1.0	Document Created
03-23-2011	Alfred Barker	1.0	Remove references to "Onity locks."
03-23-2011	Alfred Barker	1.0	Updated "Computer Center Security" with supplemental power and fault-tolerant HVAC system information.
03-23-2011	Alfred Barker	1.0	Updated "Sever Room Security (GC)" with supplemental power system information.
03-23-2011	Alfred Barker	1.0	Updated "Sever Room Security (OC)" with supplemental power system information.
03-24-2011	Alfred Barker	1.0	Secure Portal references added.
03-24-2011	Alfred Barker	1.0	Move Diagrams & Appendix information to secure portal.

Reviewers

Name	Version Approved	Position	Date
Brandon Haag	Version 1.0	Exec. Dir.	

Distribution

Name	Location
Paper Copy	Dunlap Mathis Building, Rm. 132
Original Copy	ACAD III, Rm. 175
Electronic Copy	https://portal.gsc.edu/depts/it/default.aspx

Document Properties

Item	Details
Document Title	Securing the Physical Infrastructure Plan
Author	Alfred Barker
Document Manager	Alfred Barker
Creation Date	03-13-2009
Last Updated	03-24-2012

Table of Contents

Introduction

Buildings that house Information Technology resources should be physically secure. Access to specific areas and rooms that contain Information Technology equipment should be restricted to authorized personnel. In addition to perimeter security, understanding who to contact in the event of theft, and what additional security mechanisms are in place enhance the overall security found on campus. This section will cover:

- Defining a Campus Security Methodology
- Physical Security Overview
- Cameras and Emergency Lighting
- Onity Integra Locks – Network Consideration
- Fire Controls
- Environmental Controls
- Computer Center /Sever Room Security
- Cabling Security
- Equipment Identification in the Event of Theft

Definitions

1. **GCID –** Gainesville State College Identification Number is an asset tracking mechanism used by Gainesville State College.
2. **Keycard System** – A key system by which the traditional brass cut key has been replaced with a plastic magnetic encoded credit card like access key. This card holds the users credentials, which when accessing a lock provide an auditable log.

Purpose

The purpose of the Securing the physical infrastructure plan is to supplement the *System Security Plan* with a document that has a focus on the physical security needs of the Information Technology infrastructure. These needs are the physical locking and safeguarding of the data closets and computer centers / server rooms located at Gainesville and Oconee campuses. Also addressed is the security need in identifying and protecting the power systems that services the campuses after an event has taken place, the network infrastructure that supports the communications across campus, and miscellaneous items not yet described.

Authority

Gainesville State College's Executive Council fully supports this plan. The Office of Information Technology manages and administers this plan, which is currently in effect for all of Gainesville State College, students, employees and computer systems.

Scope

This plan is in affect on both campuses of Gainesville State College.

Continuance

This plan is a living document and may be modified at any time by the Office of Information Technology or the Executive Council.

Defining a Campus Security Methodology

Currently, Gainesville State College's security methodology is one of "Defense in Depth." That is, the process of campus security is but one process found within the three-layered, seven step process – notably the "Policies, Procedures, and Awareness Layer" and "Physical Security Layer."

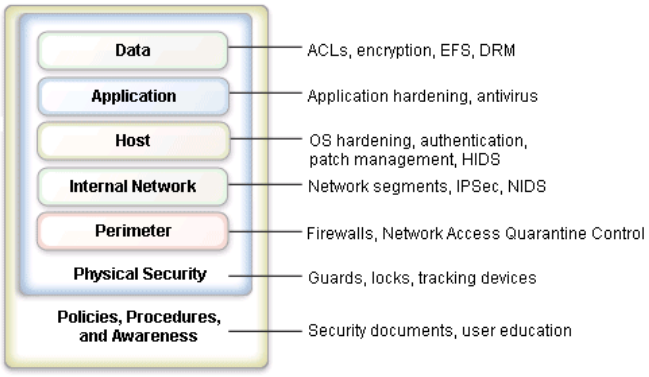

Table: Defense in Depth

Physical Security Overview (Controls)

Goals and Objectives	Milestones

All of the servers and infrastructure found on the campus are behind locked doors. The physical entry controls that are used are keys and key cards. Each member of the Office of Information Technology staff has keys or codes to enter into the below listed locations, as well as offices located throughout campus. Although this may sound secure, some custodial staff members are equipped with keys, as are the campus security officers, and Plant Operations staff.

Additional physical controls are in the form of detective and deterrent controls; detective controls are in the form of Public Safety offices, fire alarms/sprinkler systems and environmental monitors – and in some instances, camera. Deterrent controls take the form of Public Safety Officers, video surveillance cameras and the locking scheme. Protective controls, such as the presence of Public Safety Officers, the emergency lighting and the HVAC systems, must also be in place and functioning to preserve and protect personnel as well as equipment.

Campus Security Officers enhances the perimeter security by conducting campus sweeps of the buildings after the close of business. They are to record any office/area that has been left unsecured and lock any un-secured office/area.

Network equipment inventory may be referenced from the secure portal and from the office of the Director, Information Security and Network Services.

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

Note: IP numbers correspond with a device type, which assists the administrator in identifying addresses to risks and or corrupted equipment. i.e., server range, DHCP range, printer range, and wifi range…

Computer Center Security

The computer center is the heart of the administrative computing, which hosts the servers serving "Banner" and are classified as a Tier I devices. *(Reference: Incident Response Plan)* The server room is located in the Dunlap Mathis Building, Room 147, and is currently being monitored for:

- Fire – monitored by campus security
- Power – web-based monitoring with email notification…
- Temperature and Humidity
- Visual Surveillance

} *Web-Based monitoring with e-mail notifying the "Admin Group"*

This facility also hosts its own fully redundant HVAC system. All access is limited to Information Technology staff and Plant Operations and Public Safety as noted.

Entrance to the room is via the Onity Lock, which audits entry into the facility.

The external window into the facility is protected with security bars, and the internal window facing into the Executive Director's office is double-pane shatter-proof glass, and the walls surrounding the facility go completely to the ceiling to enclose the space.

This facility's power is fully supported with fault-tolerant natural-gas generator, which powers-up automatically when the main is tripped. All of this facility's systems and controls are included.

The room is protected with a water-based sprinkler system and HALON fire extinguisher located just outside of the entrance.

Server Room Security (GC)

The Server Room is the heart of the academic computing, which hosts the Windows servers serving "e-mail, web, home folder, shared classes, and Domain Controllers" and are classified as a Tier I, II and III devices. *(Reference: Incident Response Plan)* The server room is located in the A3 Building, Room 174, and is currently being monitored for:

- Fire – monitored by campus security
- Power – web-based monitoring with email notification…
- Temperature and Humidity
- Visual Surveillance

} *Web-Based monitoring with e-mail notifying the "ServerRoom Group"*

This facility also hosts its own HVAC system. All access is limited to Information Technology staff and those in Plant Operation and Public Safety as noted.

Entrance to the room is via the Onity Lock, which audits entry into the facility.

The external window into the facility is protected with security bars.

This facility's power is fully supported with fault-tolerant natural-gas generator, which powers-up automatically when the main is tripped. All of this facility's systems and controls are included.

The room is protected with a water-based sprinkler system and HALON fire extinguisher located just inside of the entrance.

Server Room Security (OC)

The Server Room is the heart of the academic computing at the Oconee Campus, which hosts the Windows servers serving home folders, backup and bookstore servers, and Domain Controllers" and are classified as a Tier I, II, and III devices. *(Reference: Incident Response Plan)* The server room is located in the OC3 Building, Room 506, and is currently being monitored for:

- Fire – monitored by campus security
- Power – web-based monitoring with email notification…
- Temperature and Humidity
- Visual Surveillance

} *Web-Based monitoring with e-mail notifying the "ServerRoom Group"*

This facility also hosts its own HVAC system. All access is limited to Information Technology staff and those in Plant Operation and Public Safety as noted.

Entrance to the room is via the Onity Lock, which audits entry into the facility.

This facility's power is fully supported with fault-tolerant natural-gas generator, which powers-up automatically when the main is tripped. All of this facility's systems and controls are included.

The room is protected with a water-based sprinkler system and a hand-held extinguisher inside the entrance.