*Information Security Policy*

# Purpose

The Information Security Policy outlines and defines the elements and controls that support John A. Gupton College databases, systems, processes, and safeguards. The policy ensures that the institution:

* Establishes a comprehensive approach to information security
* Establishes safe practices for protection and security controls
* Develops awareness procedures for faculty, staff, students, and guests
* Develops response for breaches of information security

The Information Security Policy is intended to help protect any information that is deemed sensitive or confidential. The policy applies to information that is stored or shared in anyway, which includes electronic information, information on paper, and information shared orally or visually (such as telephone or video conferencing).

# General Policy

John A. Gupton College prohibits unauthorized access to college assets. John A. Gupton College prohibits using assets to violate any laws or breach of confidentiality to authorized users. John A. Gupton provides awareness training, education, and compliance in policies and procedures related to the security and protection of information. The College recognizes that no single office, policy, or procedure provides absolute security; there all College employees and authorized users are responsible for minimizing risks and securing information within their control. The College will take appropriate action, as needed, to respond to any breach or violation of the Information Security Policy.

John A. Gupton College encourages policies and practices that help manage information systems and in securing PII. Personally Identifiable Information (PII) is an asset to protect from breaches in security. Below illustrates the Plain PII (inner circle) and the Sensitive PII (outer circles). Personally Identifiable Information (PII) is any information about an individual maintained by an agency. This information is usually the general information such as name, address, email address, and phone number. The Sensitive Personal Identifiable Information is information that could cause substantial harm, embarrassment, inconvenience, or unfairness to an individual.

# Employee Use policy

John A. Gupton College makes computer systems available to employees to perform their work. The College owns the computers and provides a server to ensure connections are valid and wireless connections can be made. John A. Gupton supports the use of technology to enhance the academic and administrative needs of all students, faculty, and staff. Personal use of technology resources is permissible as long as it does not interfere with job responsibilities and is not excessive. John A. Gupton College website is updated by approved staff members and is hosted by a contracted vendor for additional security.

**EMAIL**

John A. Gupton College provides email addresses for all staff and some faculty. The email addresses are issued at time of hire and are provided through Google Apps for Education. These accounts are for the sole use of the employee. Accounts are not transferrable and employees are responsible for keeping a secure password, ensuring confidentiality of login, protecting the information on the computer, in addition to the printer and copier. Employees may not access or alter any file belonging to another user without his/her permission. The College reserves the right to inspect email and files and take appropriate action as needed. Employees should not knowingly forward virus-infected emails to others.

**DATA SECURITY/PASSWORDS**

Data Security is protected by passwords. John A. Gupton College encourages all users to ‘protect the password’. All users for the email system and the SonisWeb system of John A. Gupton College is password protected. Each individual has a user name and user password that is unique to each system. Changes to passwords are encouraged periodically as well as the strength of the password itself. John A. Gupton College users are encouraged not to reveal their personal passwords, never to email passwords to others, and never use the same password for multiple accounts.

# SonisWeb Policy

SonisWeb is a complete online Web system. SonisWeb provides options for setting specific defaults such as billing options, registration period dates, login options, and options for instructors for syllabi storage, as well as many more alternatives. SonisWeb is used by faculty, staff, students, and alumni. To access the web-based system you must have a user name and password. To receive a user name and password, you must be registered as an applicant, student, faculty, or administrative staff. SonisWeb is operated by Jenzabar and utilizes their own server for security.

# Retention/Destruction Policy

John A. Gupton strives to uphold all materials that are private by ensuring retention and destruction policies. The Registrar keeps the retention schedule of documents. The College has a contract with Shred-It to dispose and shred documents every three (3) months. The retention schedule of the college is also based on the Accrediting Agencies policies on retention.

# Security Breach Policy

The Security Breach Policy applies to John A. Gupton College and any third party contractors working with the College. Security breaches must be reported to Administration immediately. A breach being defined as any unauthorized access to information regarding employees, students, or alumni. John A. Gupton College is responsible for investigating all security breaches. Any violations or consequences of the violation is the decision of the President of John A. Gupton College.

# Systems Security Responsibilities

John A. Gupton College is the owner of all the information systems of the College. The College is responsible for the infrastructure and ensuring all network and software programs are secure and maintained to provide confidentiality, and integrity. The responsibility for the systems security for John A. Gupton College is all users. Each employee has a password protected computer, in addition to a password protected email. The system for John A. Gupton College is protected by Carbonite and is backed up daily.

The college asks that when using a flash drive they are password protected if any vital or private information is held on them by faculty and staff.

# Training

All new employees of John A. Gupton College must participate in training of the importance of information security. All employees who handle Sensitive PII are required to undergo annual security training.