JOHN A. GUPTON COLLEGE

Information Security Policy

1 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 any way, which includes electronic information, information on paper, and information shared orally or visually.

2 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 confidentiality to authorized users. John A. Gupton College provides awareness training, education, and compliance with policies and procedures related to the security and protection of information. The College recognizes that no single office, policy, or procedure provides absolute security; that 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 (the 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. Sensitive Personal Identifiable Information is information that could cause substantial harm, embarrassment, inconvenience, or unfairness to an individual.


Date of Birth
Plain PII
*Name
*Address
*Email Address
*Phone Number
Criminal History
Last 4 digits of Social Security Number
Medical Information

3 DATA SECURITY

Data Security is protected by passwords. John A. Gupton College encourages all users to 'protect the password'. All users for the email system and all learning management systems of John A. Gupton College are 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.

4 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 of and shred documents every three (3) months. The retention schedule of the college is also based on the Accrediting Agencies policies on retention.

5 DISASTER RECOVERY PLAN

In the case of any emergency, John A. Gupton College has goals to minimize any disruption of normal operations for the students. All records are maintained in perpetuity and secured from theft, alteration, and damage. Current student records are maintained in a locked file room in a fire-resistant cabinets. Complete backups of official student academic records including transcripts, officially signed grade records, and graduation lists are secured on CD Rom files in a fireproof file cabinet and housed in a safety deposit box maintained off campus at Renesant Bank, West End Avenue Branch. All other student and institutional records will be maintained for at least 5 years after graduation or the date of last attendance. In the event of unanticipated closure of the institution, all records are kept by the accreding agency, The American Board of Funeral Service Education, located in Woodbury Heights, New Jersey.

6 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 is 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 are the decision of the President of John A. Gupton College.

7 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 system's 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.

8 TRAINING

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