Policy Number: 606
Policy Title: Data Classification and Handling Policy
Policy Council Review Date(s): 6/27/14
PPAB Approval Date:

POLICY:

Georgia Perimeter College’s information and supporting technology assets will be classified according to sensitivity and criticality and will be handled and protected in accordance with those classifications.

PROCEDURE:

This policy applies to all information assets including data, applications, processing systems, and communications equipment. All assets will be assigned an owner. Owners are assigned responsibility and accountability for ensuring that assets are appropriately evaluated and classified. The Office of Information Technology will assist in the process and will ensure that appropriate security practices and measures are maintained. All users are responsible for handling information consistent with this policy.

Sensitivity Classification

All data have varying degrees of sensitivity, which refers to either confidentiality or integrity issues. Sensitivity classifications will designate the level of security and type of handling needed to protect the confidentiality and integrity of the data. It is the responsibility of the data owner to determine the level of sensitivity. Three categories of information sensitivity are defined: Public, Internal Use Only, and Restricted. Definitions and general guidelines for sensitivity classifications are as follows:

I. Public Information:

Public information is information that if made widely available inside and even outside the college would have no detrimental impact on the college. Public information has no security restrictions or markings to indicate a sensitive nature. Public use of this information does not conflict with legal or regulatory requirements, such as Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), and the Open Records Act of Georgia. Examples of information available to the general public include course schedules, course summaries, office contact information of faculty and staff, and GPC authorized public bulletins. No special storage, transmission, or disposal requirements are specified for Public Information except where GPC document retention requirements are relevant.
II. Internal Use Only Information:

Internal Use Only information includes data that if inappropriately disclosed or accessed could negatively impact the effectiveness of GPC’s operation, expose the college to civil liability, or result in damage to reputation and public confidence. Information designated as Internal Use Only will be secured with access limited to authorized users of the information based on need to know. Internal Use Only information stored on workstations, laptops, voicemail, and other storage media maintained by the college must be password protected in accordance with the Policy 507 Appropriate Use of IT Resources and Policy 612 Password Management. Internal Use Only paper documents should be destroyed and electronic documents should be permanently deleted from storage media. All documents disposed of must meet document retention requirements as determined by the institution and pursuant to federal, state, and local regulations.

With regard to FERPA and student education records, Internal Use Only information includes the following:

- Student Grades
- Class lists
- Student Course Schedules
- Disciplinary records
- Student financial records
- Payroll records for employees who are employed as a direct result of their status as students (e.g. work study, assistantships, resident assistants)

Information that is personally identifiable (that can personally identify an individual, resulting in the risk of identity theft) or exposes the college to possible fraudulent activities is considered Restricted Information.

III. Restricted Information:

Restricted information requires the highest degree of protection based on its sensitivity, including requirements for compliance with applicable laws, regulations, and industry practice (e.g., Health Insurance Portability and Accountability Act, Gramm Leach Bliley Act, identity theft laws). Inappropriate disclosure, access, or use of Restricted Information could have substantial negative impact on the college including fines or other sanctions for non-compliance with laws and regulations, significant damage to the college’s reputation and public confidence, and critical disruption of college services. Restricted information includes the following types of data:

- Social Security Numbers;
- Passwords and PINS;
- Driver’s License Numbers;
- Banking account numbers and PINs;
- Payment card numbers (debit and credit);
- Magnetic strip information on payment cards (CVV, CVC2, PIN values);
• Individual financial information such as account numbers, credit checks, and scores;
• Individual medical condition, treatment, and/or account information;
• Data that exposes the college to possible security related or fraudulent activities (e.g., system passwords, user passwords, sensitive technical information, etc.);
• Any data that is required by law or regulation to be treated with this level of security and protection (e.g., HIPAA-covered medical information);
• Personally identifiable information (any combination of data elements that allow a person to be individually identified, such as name and address, Social Security Number, Driver’s License Number, date of birth, financial account numbers, etc.).

Access to Restricted information is granted based strictly on job duty assignment and need to know. The information is to be shared with only those parties who can effect an advancement of the task at hand, such as processing an employee or student file or maintaining a GPC asset. Restricted documents must be stored securely if in paper format or in password protected systems if in electronic format. Restricted information must never be stored on removable or portable media.

As technology permits, encryption is required for selected restricted data elements both in transit and in storage, including but not limited to the following:

• Social Security Numbers and Federal ID Numbers;
• Payment card numbers (debit and credit);
• Magnetic strip information on payment cards (CVV, CVC2, PIN values);
• Banking account numbers and PINs;
• Protected health information including immunization records;
• Driver’s License Numbers;
• Passwords and PINs;
• Encryption keys;

It is preferred that Restricted data not be stored on computing devices unless absolutely necessary for the performance of job duties. When Restricted or sensitive information has to be stored on computing devices, the device user must ensure encryption is enabled to protect the information. Computing devices include desktop, laptop, and tablet computers and smartphones. The devices must be configured such that any sensitive data stored will be encrypted at all times. Users shall work with IT or Information Security to have the encryption properly installed and configured for sensitive data protection.

Restricted information must be disposed of in permanent, unrecoverable ways. Paper documents must be destroyed or stored securely until destroyed. Electronic data must be permanently and completely deleted from any media. Data on computers that are being repurposed should be removed using Department of Defense (DoD) approved wipe procedures. If computers are being retired, hard drives should either be physically destroyed or certified as completely cleaned (to DoD wipe standards) by a qualified third party. All documents disposed of must meet document retention requirements as determined by the institution and pursuant to federal, state, and local regulations.
Unauthorized sharing, acquiring, using, or disposing of Restricted Information is considered a serious violation of this policy. Reports of violations will result in investigation and a range of possible sanctions for confirmed violations. Some violations may constitute criminal offenses, as outlined in local, state, and federal laws. GPC will carry out its responsibility to report such violations to the appropriate authorities.

**Criticality Classification**

Data and information resources are classified in terms of criticality based on the impact that their unavailability would have to the college’s operations. Criticality classifications indicate requirements for recovery in the event of service interruptions. Data owners are responsible for evaluating criticality of information resources with assistance from OIT and information security personnel as needed.

**Asset Types:**

All information assets will be organized into the following categories:

- Data
- Equipment/Hardware
- Software
- Personnel
- Facilities
- Operations

**Classification Categories:**

All information assets will be evaluated and classified to a tier grouping. The tier groupings are based on the potential impact of an outage on college operations. The classification tiers are defined as:

- Tier I – Critical Assets
  College could not operate without the asset.
- Tier II – Very Important Assets
  College could operate a few days without the asset
- Tier III – Important Assets
  College could operate in a limited fashion for an extended period of time without the asset

**Data Ownership**

All data and information assets will be assigned an owner. An Information Owner refers to the person who has the ultimate authority and accountability for the information assets in his/her functional area, usually a senior management person such as the head of the business function or department. In general, Information Owners are responsible for ensuring appropriate protection of the information resources to which he or she is assigned ownership. Ownership is usually designated to the functional area where the data originates or where it is primarily used.

Owners are responsible for ensuring that assets in their area of responsibility are evaluated and classified according to both sensitivity and criticality. OIT and information security personnel will
provide assistance and facilitation as needed. Information Owners have other responsibilities related to security of their information. Please refer to Policy 611 Information Security Roles and Responsibilities for additional information.

**Compliance and Enforcement**

Staff, faculty, and students are required to comply with this policy. Persons in violation of this policy are subject to a range of sanctions, determined and enforced by GPC management, including the loss of computer network access privileges, disciplinary action, dismissal from the college, and legal action. Some violations may constitute criminal offenses, as outlined in the Georgia Computer Systems Protection Act and other local, state, and federal laws. The college will carry out its responsibility to report such violations to the appropriate authorities.