Policy Number: 600

Policy Title: Access Control

**POLICY:**

Georgia Perimeter College will control user access to information assets based on requirements of individual accountability, need to know, and least privilege.

**PROCEDURE:** [This is policy, not procedure.]

Access to the GPC’s information assets must be authorized and managed securely and in compliance with appropriate industry practice and with numerous applicable legal and regulatory requirements (e.g., the Health Insurance Portability and Accountability Act, Family Educational Rights and Privacy Act, the Open Records Act of Georgia, Gramm Leach Bliley Act, and identity theft laws).

GPC information assets include data, hardware and software technologies, and the infrastructure used to process, transmit, and store information. Any computer, laptop, printer or device that an authorized user connects to the campus network is subject to this policy. Authorized users accessing college computing resources and network with their own personal equipment are responsible for ensuring the security and integrity of the systems they are using to establish access.

**Access Controls**

Access to information assets must be restricted to authorized users and must be protected by appropriate physical, administrative, and logical authentication and authorization controls. Protection for information assets must be commensurate with the classification level assigned to the information. Each computer system shall have an automated access control process that identifies and authenticates users and then permits access based on defined requirements or permissions for the user or user type. All users of GPC systems must be accurately identified, a positive identification must be maintained throughout the login session, and actions must be linked to specific users. Access control mechanisms may include user IDs, access control lists, constrained user interfaces, encryption, port protection devices, secure gateways/firewalls, and host-based authentication.

**User Identification, Authentication, and Accountability**

**User IDs:**

The access control process must identify each user through a unique user identifier (user ID) account. User IDs are assigned by the Office of Information Technology and application support personnel. Users provide their user ID at logon to a computer system, application, or network.
Individual Accountability:

Individual accountability must be maintained. Each and every user ID must be associated with an individual person who is responsible for its use.

Password Authentication:

Authentication is the means of ensuring the validity of the user identification. All user access must be authenticated. The minimum means of authentication is a personal secret password that the user must provide with each system and/or application logon. All passwords used to access information assets must conform to GPC requirements relating to password composition, length, expiration, and confidentiality. Please refer to Policy 612 Password Management for additional requirements.

- Passwords that are assigned by the system or administrator (e.g., for new accounts, forgotten passwords) should be initially set as a one-time use password if technically feasible, requiring the user to assign their own password at their next logon.
- Access to password authentication data should be restricted and protected with access controls and one-way encryption.
- Authentication data transmitted over public or shared data networks must be protected.
- Authentication data should be protected as it is entered into the system, including suppressing the display of the password as it is entered.
- Vendor or system assigned default passwords must be changed on first use.
- All passwords should be at least eight characters in length. For privileged access, including database, operating system, and access to restricted information, passwords of at least ten characters in length should be used.
- Applications and systems should require complex passwords, consisting of three of the following four criteria: upper case alphabetic, lower case alphabetic, numeric, and special characters (punctuation symbols, math symbols, etc.). When possible, use of all four criteria is recommended (not all systems will accept special characters).
- Applications and systems should require that new passwords cannot be the same as the four previously used passwords.
- Applications and systems should require that passwords, including user, service, and process accounts, be changed at a maximum of every 120 days. Users who process or access Restricted information (such as protected health information, student FERPA data, and Social Security Numbers or other personally identifiable information) should change their passwords at least every 90 days. Passwords for privileged accounts, including system administrator, database administrator, and accounts accessing restricted information, should be changed at a maximum of 60 days.

Access Privileges

Each user’s access privileges shall be authorized on a need-to-know basis as dictated by the user’s specific and authorized job functions. Authorized access will be based on least privilege. This means that only the minimum privileges required to fulfill the user’s job functions will be permitted. For example, if only view access to data is needed, the user should not be provided
with write privileges. Access privileges must be defined so as to maintain appropriate segregation of duties to reduce the risk of misuse of information assets. Any access that is granted to data must be authorized by the appropriate Information Owner (refer to Policy 606 Data Classification and Handling for more information on Information Owners).

Access privileges should be controlled based on the following criteria, as appropriate:

- Identity (user ID);
- Job assignment or function;
- Physical or logical locations;
- Time of day/week/month;
- Transaction based access;
- Service constraints;
- Access modes such as read, write, execute, delete, create, or search.

Privileged access (e.g., administrative accounts, root accounts) must be granted based strictly on job requirements. The number of personnel with special privileges should be carefully limited.

**Access Account Management**

User ID accounts must be established, managed, and terminated to maintain the necessary level of data protection. The following requirements apply to network logons as well as individual application and system logons, and should be implemented where technically and procedurally feasible:

- Account creation requests must specify access either explicitly or via a “role” that has been mapped to the required access. New accounts created by mirroring existing user accounts must be audited against the explicit request or roles for appropriate access rights.
- Accounts must be locked out after five consecutive invalid logon attempts. When a user account is locked out, it should remain locked out for a minimum of five minutes or until a System Administrator unlocks the account.
- Accounts must be locked after no more than fifteen minutes of system/session idle time. This requirement applies to workstation and laptop sessions as well as application sessions where feasible. The Office of Information Technology will implement measures to enforce this requirement and to require the user to re-authenticate (enter password) to reestablish the session.
- Systems housing or using restricted information must be configured in such a way that access to the restricted information is denied unless specific access is granted. Access to restricted information is never to be allowed by default.
- Access must be revoked immediately upon notification that access is no longer required. Access privileges of terminated or transferred users must be revoked or changed as soon as possible. In cases where an employee is not leaving on good terms, the user ID must be disabled simultaneous with departure. Access for users who are on leave of absence or extended disability must be suspended until the user returns.
- User IDs must be disabled after thirty days of inactivity for employees. After an additional thirty days, the employee user ID will only be available for reactivation with management approval. Student IDs will be disabled after a period of inactivity that is determined appropriate by the current business process. These requirements may not apply to certain specialized accounts (e.g., NT Admin, root). In those instances, the System Administrator must provide a written waiver to Information Security and document the compensating controls around access to the accounts.
- All third party access (contractors, business partners, consultants, vendors) must be authorized and monitored. Third party access to information assets will be granted in increments of three, six, nine, or twelve months as needs dictate. In cases where access is needed for longer periods, the business function management must specify access time frame and justification for such access.
- Appropriate logging will be implemented commensurate with sensitivity/criticality of the data and resources. Logging for accounts must include failed logons. Where practical, successful logons to systems with restricted information should be logged. Logs should be monitored and regularly reviewed to identify security breaches or unauthorized activity. Logs should be maintained for at least ninety days.
- A semi-annual audit of computer resource authorizations to confirm that access privileges are appropriate must be conducted. The audit will consist of reviewing and validating that user access rights are still needed and are appropriate.

**Compliance and Enforcement**

The policy applies to all users of information resources including students, faculty, staff, temporary workers, vendors, and any other authorized users who are permitted access. 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.

PPAB Approval Date: ________________________________

Policy Council Review Date(s):

ITPC: 8/24/12