Policy Number: 501
Policy Title: Web Server Infrastructure

**POLICY:**

General oversight of the Georgia Perimeter College Web servers and Web pages, and policies governing the use of these resources, is the responsibility of the Chief Technology Officer.

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

GPC is responsible for providing a secure and reliable college network. The Office of Information Technology (OIT) shall be responsible for providing services for the scope of this policy. This will be accomplished by the use of college-wide network and server standards and limiting access to network connections that do not conform to this document. The policy governs the use of electronic communications resources.

**OIT Responsibility**

Personal Web pages are individual Web pages sponsored and maintained solely by students or by members of the Georgia Perimeter College faculty or staff but that are not directly connected with the Georgia Perimeter College mission. Georgia Perimeter College is not responsible for personal pages. Georgia Perimeter College reserves the right, however, to remove from any GPC Web server, any page or link in violation of the law or college policies.

All Web servers associated with Georgia Perimeter College must be registered with the Office Information Technology. Registry information is submitted through the Web Server Registration page (http://facstaff.gpc.edu/personalwebsites/).

Information will be stored by the Office Information Technology and verified periodically.

All Web service providers are responsible for the currency, legitimacy, legality, and appearance of their pages. Also, Web service providers must adhere to GPC’s Web policies. Content owners are responsible not only for the content and appearance of their own pages and be responsible for any linked personal pages which branch from their pages.
The Division of Infrastructure Technology manages the resources and technical issues regarding Web accounts, college servers, and system configurations. IT also oversees all aspects relating to maintenance of the main GPC Web servers and supporting infrastructure.

**Hardware Servers**

Official pages must reside on secure servers and must comply with the following:

- The only users permitted login accounts to these servers are those authorized by the server’s owner (or designee) at the request of an official page owner.
- These servers must have redundant power supplies and be connected to an uninterruptible power supply. They must be configured with mirrored system disks and redundant disks.
- System administrators are responsible for maintaining software at a patch level that is appropriate for their environment and that protects the rest of the campus.
- OIT will periodically run scans of systems within the firewall and work with system administrators to identify changes needed to keep their systems secure.
- Secure servers must be kept on a regular and appropriate backup schedule, as defined in the unit’s Business Continuity Plan. The backup media must have a retention schedule and off-site storage procedures that comply with their unit’s Business Continuity Plan.
- Secure servers must be within the GPC firewall or, if they are outsourced, the service provider must by contract meet these requirements.

Non-official pages can be hosted on any server, secure or insecure, and must comply with the following:

- No official pages are allowed on insecure servers.
- Content owners may set their own policies on to whom they give login access.
- OIT will periodically run scans of systems within the firewall and work with system administrators to identify changes needed to keep their systems secure.
- They are subject to the Acceptable Use and Privacy policies.

**Managing the GPC.edu Domain and its sub-domains**

Root Level Directories are determined and assigned by the Assistant Director of Infrastructure Technology.

Names must adhere to GPC’s naming conventions for Short Site Names and Webview Publish URLs.
The Assistant Director of Infrastructure Technology will maintain a current site map and current links for official pages. Disputes about links will be settled by the Chief Technology Officer and Web Policy Committee.

**Leaving GPC**

It is the responsibility of any page owner leaving GPC to copy and remove any unofficial page material. This includes faculty members who have left GPC and are not officially on leave, staff members who have left, and students who are no longer enrolled.

Login accounts to servers will be disabled under existing OIT policies, i.e., at the time a person leaves GPC.

After a six month period, **immediately upon separation from the college**, system administrators **may** delete these pages and are not responsible for archiving them. GPC will not be responsible for any deleted material.

[AAPC: A procedure needs to be in place for personal webpages to be immediately deleted by OIT when any employee is officially separated from the college, except for the provision made below. Otherwise, former employees are able to misrepresent their status with the college for a lengthy period of time.]

At the request of a Dean, an exception will be made for faculty which will be left linked to the school or college for the length of time specified by the Dean.

At the request of a faculty member, an exception will be made for student materials (e.g. portfolios), which will be left linked to the school or college for the length of time specified by the faculty member.

**Compliance and Enforcement**

The policy applies to all GPC employees. 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):