

Computing and Information Services – Fred Miller, Chief Information Officer

Title: Web Standards and Security Measures Policy

Applicable: Furman University [Students, Staff and Faculty]

Contacts: Computer Help Desk ext. 3277

Background: As the use of web technologies increase on Furman's campus, it has become necessary to create a policy that states Furman's web standards and preferred security measures.

Policy: All campus web services and sites that transmit or receive unique user input via forms or other technologies should be implemented with industry standard encryption. Before web sites are posted or technologies implemented, the security requirements should be considered. Systems that allow for generic or anonymous posting should be implemented with features or additional modules that allow for protection against spam and other abuse trends. New technologies will be considered based on the possible need to integrate with our portal technology.

Guidelines:

- a. All campus web services and sites that transmit or receive unique personal identifying user input via forms or other technologies should support and as appropriate be implemented with industry standard encryption (SSL). Along with the implemented encryption, users should apply best practices for these methods if they are selected campus solutions.
- b. Before web sites are posted or technologies implemented, the security requirements should be considered and implemented with technologies that will meet the needs both from the perspective of the protection of Furman University and that of the web users' protection and privacy.
- c. Initial needs do not always indicate future needs, web systems that do not have current needs for encryption does not imply there is no future need for encryption.
- d. Web technologies are required to employ adequate encryption if they are accepting or distributing usernames, passwords or other appropriate-for-securing information.
- e. Newly implemented web-based technologies such as blogging, bulletin boards, guestbooks, and other systems that allow for generic or anonymous (no unique per-user login credentials) posting should be implemented with C&IS approved features or additional modules that allow for protection against spam and other abuse trends (Ex, captchas). Guids, cookies, web bugs, ip addresses or other pseudo-anonymous systems that do not require end-user registration or account assignment are considered "anonymous" in the context of this requirement
- f. Where applicable, privacy policies should be developed, followed in practice, and available for web users to review prior to employing use of the system in question.
- g. Users implementing new web sites are advised of the importance of encrypting all logins (regardless of the content of the material made accessible via the login). This offers some protection for the University from users who recycle their passwords for secured systems with those for insecure systems.
- h. Basic auditing should be available, and implemented where appropriate, for newly implemented web solutions, particularly for those that employ unique users. The extent of the auditing requirements is dependent on the application and resources assigned.

- i. Newly implemented technologies will be considered based on the possible need to integrate with our portal technology. Attention should be given to appropriate authentication methods currently Ldap (recommended) or radius (backup) that allow existing security infrastructure without unnecessary increase in security or integration costs.
- j. Existing technologies should be upgraded or moved to platforms that support these goals.
- k. All special requests must be approved by Furman's Chief Information Officer.