Secure Web Application Development / FIN-ITS-007

I. Purpose of the policy

This policy defines requirements for Web application development and security for all PSU Web applications deployed on or off-campus.

II. Applicability and Authority

This policy applies to any Web-based technology purchased, obtained at no cost or developed in-house, hosted locally or cloud-based.

III. Detailed Policy Statement

It is the responsibility of Web application developers and their supervisors to follow Web application development and security standard policies. This policy focuses on Web application development standards and is intended to complement patch management, server management and change management.

See the Sensitive and Confidential information policy for definitions for Sensitive and Confidential.

- Encryption
    i. Valid Transport Layer Security/Secure Sockets Layer (TLS/SSL) certificates must be used for all sensitive information in transit between the client, server and other servers
    ii. Production services that use TLS/SSL certificates must obtain them from a recognized Certificate Authority (CA)
    iii. Applications using cryptography must use industry standard algorithms and implementations
- Authentication and Authorization

i. CAS or other ITS approved industry standard sign-on technology (such as Shibboleth) backed by Active Directory or other ITS approved directory service must be used to authenticate PSU users
ii. If CAS cannot be used, then the PSU Active Directory or other approved directory service must be used.
iii. Web applications that process sensitive data must verify authorization for each request
iv. Authorization data shall be stored in Active Directory, APE or other ITS approved Directory Service

- Data Validation
  i. Web applications must validate all data for expected values
  ii. Web applications must use server-side validation
  iii. Web applications that use data from another source must take steps to ensure the external data is trustworthy
  iv. Web forms and interactive elements must use a secure token to verify the user intentionally initiated the request
  v. Web applications must validate all data that is passed to interpreters, including Web browsers, database systems and command shells
  vi. Web applications must only send data and code to the browser that the user is authorized to see or use
- Session management
  i. Web applications must set the 'secure' flag for cookies that contain sensitive data to ensure they are only sent over secure connections
  ii. Web applications must keep session times to the minimum duration necessary for operation
  iii. Web applications must have server-based disconnects
  iv. Web applications must use a secure session key/token to avoid sending 'hidden data' to the browser

IV. Procedures

Web Applications at Plymouth State University are to be developed according to standards and best practices set forth by ITS. Developing to standards allows for any developer to quickly review work for any potential problems – including those revolving around security.

- Developers use standardized and uniform code to establish secure access to databases using abstraction code libraries in a manner consistent with industry standards.
- Authentication tokens shall expire consistent with inactivity timeouts established for user sessions.
- Developers will write code with the intent of making it easy to maintain.
- Authorization for web application access is validated on every page load.
- Authorization are handled using a standard methodology within an application.
- The full coding standards document can be found at https://www.plymouth.edu/webapp/mis/wiki/Coding_standards

V. Non-compliance

Members of the PSU community who violate this policy will be subject to disciplinary action, up to and including termination of employment.

VI. Definitions

CAS Central Authentication Service provided by ITS.

VII. Related Policies / References for More Information

- Acceptable Use Policy
- Email Use Policy
- Sensitive and Confidential Information Policy-
- User Credentials Policy