University of Colorado Boulder	**University of Colorado Boulder** **Campus IT Policy**

Effective:	March 4, 2015
Responsible Office:	The Office of the AVC for IT and CIO
Policy Title:	Policy for Web Site and Web Application Security
Approved	Philip P. DiStefano, Chancellor

Purpose:

Establish technical and procedural standards for development of web sites and *web applications* for CU-Boulder entities to ensure consistency with the Retention of University Records and Information Security Program APS.

A. Introduction

The Information Security Program APS establishes requirements for the campus Chief Information Officer and IT service providers. Specifically, the Chief Information Officer is charged with enforcement of university and campus policies relating to information technology and information security. All IT service providers have the responsibility to implement security safeguards to protect university information and IT resources. These safeguards are necessary to protect University information from inappropriate access, disclosure and misuse; provide assurances that information resources are available as needed for University business; and comply with applicable policies, laws, regulations, rules, grants, and contracts.

The Retention of University Records APS requires University records be maintained in a medium owned or controlled by the university. If the University does not offer a practical solution, (as determined by the campus chief information officer) records may be maintained on outsourced information technology (IT) services (such as web sites, web-based documents or social media sites), as long as departments seek approval from the campus information security officer (ISO) to ensure that vendor contracts and/or terms of service meet University standards.

B. Content

The following standards apply to all Boulder campus web sites and *web applications*:

- *Internet facing web applications* not leveraging the campus web environment or OIT supported infrastructure must have hosting and management solutions reviewed by campus Information Security Office.
- *Web applications*, web sites and the underlying infrastructure will be subject to regular OIT security

scans or audits.

- Any authentication or authorization needs will use a method approved by the campus ISO. OIT will publish, in consultation with campus IT governance, a list of pre-approved methods, by April 2015.
- To mitigate risk of permanent data loss from natural causes, building failures, or malicious acts highly-critical applications (as defined in the Standards for Data Classification and System Security Categorization) must be physically located in a secure data center as approved by the campus ISO.
- A university employee will be identified as the application owner and will be the primary contact when application support or security questions arise. Departments have the responsibility to notify OIT Security when contact information changes or when employees leave the University.
- Application developers must complete the CU Skillsoft Secure Application Development training or demonstrate sufficient knowledge through either a test or professional certification.
- Application owners will be sent a Docusign document to certify their responsibilities and attest to compliance with relevant policies annually.
- For highly-critical or highly-confidential (as defined in the Standards for Data Classification and System Security Categorization) systems the campus ISO will assess the security controls in the information system and its environment of operation annually to determine the extent to which the controls are implemented correctly

C. Administration and Enforcement

Any deviation from these standards must be approved by the campus AVC for Information Technology and CIO. Exceptions shall be recorded by OIT and reviewed annually. The AVC for Information Technology and CIO will have the responsibility to review and update these standards annually. Units requesting an exception should initiate the exception process by contacting the IT Service Center.

D. Definitions

- Web Application - application software utilizing a web browser as the user interface and created in a web browser supported programming language.
- Internet Facing – refers to computer systems which are accessible **from** the Internet.

E. Selected References to University Policies.

- Information Security Program - http://www.cu.edu/ope/aps/6005
- Retention of University Records - http://www.cu.edu/ope/aps/2006
- Standards for Data Classification and System Security Categorization - http://www.cu.edu/sites/default/files/CUdataclassification.docx
- Accessibility Policy – TBD
- CU Branding and Identity Standards - http://www.cu.edu/brand-and-identity-guidelines/cu-branding-and-identity-standards-manual

F. Responsible Organization

The Office of the AVC for Information Technology and CIO will be responsible for this policy.