THE UNIVERSITY OF CHICAGO MEDICINE & BIOLOGICAL SCIENCES

BSD Security Standards for Web Applications

Standard	STA-07	Effective Date	DRAFT as of 08/18/2015	Modified Date	09/01/2015	Version	1.0

Table of Contents

PURPOSE

This document defines the BSD Security Standards for Web Applications required for web application that must be used to store, process or provide information owned and used by the Biological Sciences Division. These standards serve as a supplement to the University of Chicago's Guidelines for the Secure Management of IT Infrastructure Systems.

A web application owner or administrator must take steps to review and ensure that the web application is properly protected. Adherence to these standards is an essential safeguard for the protection of BSD data and systems. These standards exist in addition to all other university policies and federal and state regulations governing the protection of the university's data.

SCOPE

This standard applies to all web applications in the BSD research and academic enterprise, which includes BSD basic sciences, the Pritzker School of Medicine, and various other BSD units engaged in research. System Administrators, researchers and staff with system administration responsibilities are expected to safeguard information and systems they use and/or support. Non-compliance with these standards will result in revocation of access to the data, system, and/or network.

THE UNIVERSITY OF CHICAGO MEDICINE & BIOLOGICAL SCIENCES

STANDARD

This section lists the standards that must be enabled and enforced for Confidential and Public data. The University of Chicago Human Resource Policy 601, Treatment of Confidential Information, lists a number of different types of information, which should be treated as confidential.

If a reliable and effective solution is not available for a particular requirement, then a limited exception may be granted (see Exception section).

For the purpose of this document a "web application" is an application utilizing web and web browser technologies to accomplish one or more tasks over a network.

1.0 Authentication and Authorization

These are the web application access control standards for authentication and authorizations.

		Data Protection Levels	
Section	**Standard**	**Confidential**	**Public**
1.1	There must be a security control mechanism to uniquely authenticate the identity of the user.	Required	Recommended
1.2	There must be a separation of access between administrative access and data access. This can be a re-authentication for administrative actions, or a secondary logon for administrative actions vs. data access actions.	Required	Recommended
1.3	Users must be assigned the least level of access needed for their function.	Required	Recommended
1.4	Applications will implement a security timeout feature. Timeouts will be set to the lowest possible level balancing the need to protect sensitive data with the usability of the application.	Required	Recommended
1.5	Applications that rely on cookies for authentication must clear any client cookies on logout of the application such that another user of that	Required	Recommended

	workstation wouldn't be able to regain entry into the application.		
1.6	Applications that do authentication must use domain or Shibboleth authentication, e.g. LDAP or Active Directory.	Required	Recommended
1.6a	Applications that manage their own accounts and passwords must follow section 1.0 of the BSD Password Management Standards	Required	Recommended
1.7	If the application has a default password, it must be changed to a unique password following the BSD Password Management Standards must before the application goes into production.	Required	Required

2.0 User Interaction

These are the user interaction standards for the web application inputs and outputs standard.

		Data Protection Levels	
Section	**Standard**	**Confidential**	**Public**
2.1	All input of any data through a web interface must be checked for validity and sanitized. Suggested order in Appendix A	Required	Recommended
2.2	Error output must be sanitized so as to not reveal too much information that can be used in an attack.	Required	Recommended
2.3	Errors and exceptions must be handled such that they will follow the same execution path as any disallowed operation.	Required	Recommended
2.4	Audit logs must be maintained within the application as specified in Appendix B	Required	Recommended
2.5	All logs must be secured and only accessible by the least privilege necessary.		

3.0 Encryption

These are the web application encryption standards.

		Data Protection Levels	
Section	**Standard**	**Confidential**	**Public**
3.1	Web applications collecting or displaying data must encrypt the data in transit using a secure version SSL that is not obsolete.	Required	Recommended
3.2	SSL/TLS Certificates must be signed by known and trusted CA, for all production application(s). The use of self-signed certificates can only be used on test or development environments.	Required	Recommended
3.3	Where a login is required for authentication and the application itself does not require encryption, the logon must happen through an encrypted mechanism such as SSL/TLS.	Required	Required
3.4	Communication with authentication provider, such as LDAP or Shibboleth, must be done through and encrypted channel such as SSL/TLS.	Required	Required

4.0 Design

These are the web application design standards

		Data Protection Levels	
Section	**Standard**	**Confidential**	**Public**
4.1	Front end for the web application may reside in a DMZ, but must be protected by a firewall.	Required	Recommended
4.2	Database must not be embedded in the application.	Required	Recommended
4.3	If the application lives in the DMZ, then the database must reside in a logically separated network from the application.	Required	Recommended

4.4	Applications that have different data protection levels should be installed on their own set of servers (physical or virtual) and not on a shared application server.	Recommended	Recommended
4.5	Threat risk modeling should be performed to fully understand the possible threats against the application being designed. See the OWASP Threat Risk Modeling Procedure.	Required	Recommended
4.6	Where possible, easily installable and portable applications should be used to allow easy reconstitution on another platform in the case of an attack or outage.	Recommended	Recommended

EXCEPTIONS

If any of the required standards cannot be met, an email, which reports the non-compliance and describes the plan for risk mitigation, must be filed with the BSD Information Security Office. To file an exception email the BSD Information Security Office at security@bsd.uchicago.edu.

RESOURCES

- BSD Information Security Office Services
- BSD Minimum Security Standards for Systems
- 601 - Treatment of Confidential Information policy
- Guidelines for the Secure Management of IT Infrastructure Systems
- The Open Web Application Security Project (OWASP)
- OWASP Threat Risk Modeling Procedure

APPROVAL AND OWNERSHIP

Responsible Office: BSD Information Security Office
Standard Owner: BSD Security Liaison Group

REVISION HISTORY

Version	Description	Revision Date	Review Date	Reviewer/Approver Name
1.0	Draft Standard	08/18/2015	09/01/2015	SLG Members

APPENDIX A – RECOMMENDED ORDER OF DATA VALIDATION

1. Decode data before performing the validation, for example check input strings to prevent the program from executing malicious commands, scripts, codes, etc.
2. Check for length criteria - for example, determine if it is within the allowable predetermined minimum and maximum range.
3. Check for acceptable data types - for example, determine if it is a valid data type (e.g., characters or numbers only)
4. Check for unacceptable data types – for example, determined whether data entered are non-characters, non-numeric, special characters

APPENDIX B – AUDIT LOGGING SPECIFICATIONS

It may not be feasible to log everything in this list, but an attempt should be made to do so

1. Logon/logoff successes
2. Security Administration changes
3. Restricted or administrative account access
4. Unsuccessful attempts to access systems or information
5. Dates and times of all of the above
6. Source information for all of the above