Scope

Indiana University Health Sciences (IUHS)

All employees and faculty of the IUHS as well as vendors, contractors, partners, students, collaborators, and any others doing business or research with IUHS, will be subject to the provisions of this policy. Any other parties, who use, work on, or provide services involving IUHS computers, technology systems, and/or data will also be subject to the provisions of this policy.

IUHS computing resources have been developed to encourage widespread access and distribution of data and information for the purpose of accomplishing the educational, clinical, and research missions of the school. This policy will not supersede any Indiana University developed policies but may introduce more stringent requirements than the university policy.
Policy Statement

1. Computer Applications should follow a standardized application lifecycle established by the manager of the application's developers. At a minimum, this should include development, testing, and production phases. Updates, patches, and feature changes should follow the same phases and processes as if the application were being developed from concept.

2. Each individual user (whether a developer, administrator, or user) should have a unique set of credentials for accessing a Computer Application. Each process or application role should also have a unique credential that is not coincident with a user.

3. Only authenticated users should have access to a Computer Application. Each user should only be allowed to access the information he or she requires. Establishing and changing access for a user or group should be approved by the Application's data owner.

4. Developers should follow best practices for creating secure applications with the intention being to minimize the impact of attacks to a Computer Application. A code validation process should be followed to discover and remediate any code errors before an application is approved for production. This may include, but not necessarily be limited to peer review and/or other methods as specified by the application lifecycle process.

5. All applications, including third party applications, will undergo application security scanning using university-provided tools and any issues identified will be remediated prior to the application being placed into the production environment.

6. The production data source should not be used to develop or test a Computer Application. Development and testing databases will be redacted if copied from production data sources. Production data sources will be stored in an encrypted format. Data in transit to and from the Computer Application will also be encrypted. A separate data source will be created for each application.

7. Web-based Computer Applications shall be hosted on secure, robust servers with multi-layered security. Application and web services error messages should be anonymized or altered to prevent exposure of coding errors, directory structure, or other information about the Application or server.

8. Logs for the server, application, and web services should be collected and maintained in a readily viewable format for a period of time specified by applicable state and/or federal regulation.
Reason for Policy

The purpose of this policy is to ensure computer applications written to support IUHS are developed using secure coding practices and follow an accepted application programming standard. Secure application coding practices are intended to reduce or eliminate the vulnerabilities and exploits with limited impact to the business.

Assumptions

It is an assumption that Computer Applications will send, receive, and store data in some type of data source. It is also assumed that the data is sensitive and would fall under the compliance effort of one or more regulatory bodies (GLBA, HIPAA, SOX, PCI-DSS, NIH, etc.). This is in opposition to Computer Applications that supply information to the public. Public applications may also send, receive, and store data in some type of data source. While the information itself is public, the management and administrative accounts, structure of the data, and other considerations make it necessary to provide similar controls for functions that are not considered public access.

Definitions

*Computer Applications* are a subclass of computer software that employs the capabilities of a computer directly and thoroughly to a task that the user wants to perform. This should be contrasted with system software, which is involved in integrating a computer's various capabilities but typically does not directly apply them in the performance of tasks that benefit the user. In this context, the term “application” refers to both the application software and its implementation.

*Secure Coding Practices* are program source code that is written to withstand attacks. The amount of effort that goes into writing a secure program is substantially greater than writing code without such concern. Normally, programmers deal with a solution to a data processing or transmission task without worrying about every line of code being a potential attack vector.

*Data Source* is a logical location where data is stored for a Computer Application. It typically refers to a database but can also be a collection of files within a directory. Its purpose is to store and exchange information with the front-end of a Computer Application.

Sanctions

If it is suspected that this policy is not being followed, report the incident to a departmental manager or representative and the Chief Information Security Officer.
Any exceptions to this policy must be approved in advance by both the Chief Information Security Officer and the Associate Vice President for Information Technology, Clinical Affairs IT Services.

Any person found to have violated this policy will be subject to appropriate disciplinary action as defined by the provisions of Indiana University Policy IT-02, Misuse and Abuse of Information Technology Resources.

---

**History**

1. IUSM SEC-01, 22 Sep 08
2. Policy reviewed on February 24, 2011
5. Policy scope edited, expanded to include Health Sciences, July 25, 2014.