Security Best Practices for Applications with Confidential University Data [1]

Application Owners are expected to know the specific types of data for which they are responsible and to make security decisions regarding access to and protection of data under their charge [2]. The following recommendations for Application Owners are applicable to all applications that handle Confidential University Data. All of the recommendations will be considered for future inclusion in official University IT Policy:

1. Ensure that all applications are coded in a secure manner that at a minimum address the vulnerabilities defined in the OWASP Top 10 list [3] (or recognized equivalent secure development guidance).
   a. OWASP contains a number of best practices, including input validation, parameterized queries and ensuring the principle of least privilege is in place for access to databases.

2. Application testing and monitoring:
   a. Regularly assess the security of applications using automated vulnerability scanning, penetration testing, and/or an IT security audit as needed (such as, prior to initial implementation, after a major code revision, upon publication of a new vulnerability, etc.).
   b. Have a defined log monitoring practice to identify unusual or anomalous behavior associated with the application and follow it.

3. Platform Testing & Monitoring:
   a. Register platforms that house highly sensitive data as a Critical Host [4]. This will result in regular platform vulnerability scanning by ISC Information Security. When notified that an application registry is available, register applications that access or store Confidential University Data.
   b. Have a defined log monitoring practice to identify unusual or anomalous behavior associated with the platform and follow it.
      i. Consider using a host intrusion detection system (HIDS) to monitor platforms housing applications with Confidential University Data to observe unauthorized or unusual activity.

4. Establish a repeatable process for responding to external notifications of current/observed attacks. This should include identifying your organization’s Security Liaison, and how they will communicate critical information.

5. Purge unnecessary sensitive data from the application regularly and move old data offline whenever possible.

6. Consider encryption for sensitive data at rest.

Note: For applications built by a 3rd party or housed on a 3rd party’s system (including ISC), data owners should work with the contracted developers and vendors to ensure that these requirements are met.

Please contact ISC Information Security (security@isc.upenn.edu or 215-898-2172) for assistance with the implementation of these recommendations.
Confidential University Data is defined in the Computer Security Policy, and includes Sensitive Personally Identifiable Information, Proprietary Information, and Other data whose disclosure would cause significant harm to Penn or its constituents:

http://www.net.isc.upenn.edu/policy/approved/20100308-computersecurity.html

Penn Data Access Standards
http://www.upenn.edu/oacp/privacy/policiesguidance/data-access-standards.html

The OWASP Top 10 list can be found here:
https://www.owasp.org/index.php/Top_10_2010

Also, for a more comprehensive list, please see the OWASP Development Guide:

Penn Critical Host Registration
http://www.upenn.edu/computing/security/crithost/index.php