a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #20
Development and Modification of Software Applications

Introduction

1. A Software Application is a piece of software designed to perform a task for end users, such as accounting, human resource management, and student information management. When purchasing, designing or substantially modifying these Applications, it is important that security requirements are understood, documented and implemented at the earliest appropriate stage of the project. This is substantially cheaper and more effective than trying to apply security controls retroactively.
2. Information Stewards/Owners are responsible for ensuring this standard is complied with whether the project is undertaken internally or by a Service Provider.
3. The Chief Information Officer has issued this document under the authority of Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

Assessing Security Requirements for Projects Involving Confidential Information

4. All new or substantially modified Applications that store or access Confidential Information must undergo a Security Risk Assessment of the new Application's security controls, using the Software Application Security Risk Assessment checklist.

Examples of "Substantially Modified":

- granting access privileges to Confidential Information to new categories or groups of individuals
- outsourcing management, storage or security of Confidential Information to an external service provider
- changing how Confidential Information is collected, used or displayed

Assessing Privacy Requirement for Projects Involving Personal Information

5. In addition to the requirement to undergo a Security Risk Assessment, all new or substantially modified Applications that store or access Personal Information must undergo a privacy impact assessment (PIA), as set out in the Privacy Impact Assessment Requirements.

Pre-Production Development and Test Environments

6. Development and test environments must be logically and/or physically isolated from any production environments.
7. Where possible, testing of new Applications should be done with fabricated data that mimics the characteristics of the real data, or on copies of real data with any Confidential or Sensitive Information appropriately sanitized. Testing should not be done on live data due to the threat to its confidentiality and/or integrity. Testing that requires the use of live data or Confidential Information must have appropriate security controls employed.

Application Development Requirements

8. Applications must validate input properly and restrictively, allowing only those types of input that are known to be correct (e.g. cross-site scripting, buffer overflow errors, SQL injection flaws, etc.).
9. Applications must execute proper error handling so that errors will not provide detailed system information, deny service, impair security mechanisms, or crash the system. See the Open Web Application Security Project for more information.
10. Where possible, code-level security reviews must be conducted with professionally trained peers for all new or significantly modified Applications, particularly, those that affect the collection, use, and/or display of Confidential Information.
11. All new or substantially modified Applications connected to the UBC network must be scanned for vulnerabilities in accordance with the Vulnerability Management standard.

Change Management

12. A change management process must be implemented and maintained for changes to existing Applications; substantial modifications may trigger a new assessment of security and privacy risks, as explained above.

System Documentation

13. University IT Support Staff must securely store system documentation and ensure that it is only available to authorized Users.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Vulnerability Management standard

Software Applications Security Risk Assessment checklist