a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD M11
Development and Modification of Software Applications

1. Introduction

1.1 When purchasing, designing or substantially modifying Software 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.

1.2 Information Stewards/Owners are responsible for ensuring this standard is complied with whether the project is undertaken internally or by a Service Provider.

1.3 The Chief Information Officer has issued this document under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Assessing Security Requirements for Projects Involving Medium, High or Very High Risk Information

2.1 Prior to storing or accessing UBC Electronic Information, complete a Software Application Security Checklist for all new or substantially modified applications that store or access Medium, High or Very High Risk Information.

2.2 All new or substantially modified applications that store or access Personal Information must also undergo a privacy impact assessment (PIA), as set out in the Privacy Impact Assessment Requirements. This PIA may require additional security assessments.

Examples of "Substantially Modified":

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

3. Pre-Production Development and Test Environments

3.1 Development and test environments must be logically and/or physically isolated from any production environments.

3.2 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 Medium, High or Very High Risk 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 High/Very High Risk Information must have appropriate security controls employed.

4. Application Development Requirements

4.1 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.).

4.2 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.

4.3 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 High or Very High Risk Information.

4.4 All new or substantially modified applications connected to the UBC network must be scanned for vulnerabilities in accordance with the Vulnerability Management standard.

5. Naming Requirements for Web Applications

5.1 Web Applications used to conduct University Business must be provisioned within the ubc.ca domain name space, e.g. widget.ubc.ca, unless not technically possible.

6. Email Requirements for Applications and ERPs

6.1 Due to the high risk of fraud and account compromise, ERPs must adhere to the following:

6.1.1 The inclusion of clickable links in unsolicited emails generated from ERPs is prohibited. In emails that are requested by the recipient, the inclusion of clickable links is not recommended. Instead, instruct Users to navigate to the ERP or website directly.

6.1.2 Use of the svc.ubc.ca managed mail subdomain service is required for all ERPs, e.g. widget.svc.ubc.ca.

6.2 The requirements in section 6.1 should be applied to non-ERP Applications unless not technically possible.

6.3 In order to make emails generated from Applications and ERPs more difficult to replicate, follow these guidelines where possible:

6.3.1 use a UBC-branded email template and remove vendor branding;

6.3.2 use customized language specific to the required action, or that defines a specific set of activities;

6.3.3 consider adding a named email signatory; and

6.3.4 include authenticating context, e.g. by providing salutations to the recipient.

7. Change Management

7.1 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.

8. System Documentation

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

9. Related Documents and Resources

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

Software Application Security Checklist

Privacy Impact Assessment (PIA)

Open Web Application Security Project (OWASP)

Vulnerability Management standard

Application Security Guidelines (with CWL credentials)