



INFORMATION SECURITY CHECKLIST

Software Applications Security Requirements Checklist

Introduction

1. Complete this checklist for all new or substantially modified applications that store or access [Medium](#), [High](#) or [Very High Risk Information](#) prior to storing or accessing [UBC Electronic Information](#).
2. This checklist has been issued by the [Chief Information Officer](#) to supplement the [Development and Modification of Software Applications](#) standard. Questions about this checklist may be referred to information.security@ubc.ca.

Security Requirements Checklist

<input type="checkbox"/>	1. A Data-Flow Map must be constructed to clearly identify UBC Electronic Information at rest and in transit: <ol style="list-style-type: none"> a. information at rest, whether being stored for use/archive or exported for reporting/analysis, must comply with the Encryption Requirements standard; and b. information in transit must comply with the Transmission and Sharing of UBC Electronic Information standard.
<input type="checkbox"/>	2. Where possible, applications must authenticate Users through central authentication systems such as UBC's Enterprise Active Directory (EAD) or CWL. If authentication will not be done through CWL or EAD then user account passwords must not be stored in clear text (see the User Account Management standard for more information).
<input type="checkbox"/>	3. University IT Support Staff must implement access controls to servers as follows: <ol style="list-style-type: none"> a. Users must be given the minimum access privileges required to perform their job function following the Principle of Least Privilege, and procedures must be enforced to authorize, add, remove, and modify user access, in accordance with the Securing User Accounts standard; b. Passphrases must be required for all accounts and must meet the requirements of the Password and Passphrase Protection standard; and c. wherever possible, access to servers should be logged in accordance with the Logging and Monitoring of UBC Systems standard.
<input type="checkbox"/>	4. Applications resident on UBC Systems that are Internet-facing must be setup in compliance with the Internet-facing Systems and Services standard.
<input type="checkbox"/>	5. To avoid data loss and ensure the availability and integrity of UBC Electronic Information stored on UBC Systems, the Administrative Head of Unit must ensure that this information is backed up regularly (typically daily or weekly) in accordance with the Backup guideline . These backups must be stored in a secure location with appropriate user access and any required encryption controls, as described in the Encryption Requirements standard.
<input type="checkbox"/>	6. If the application will be outsourced and make use of Service Providers then the Administrative Head of Unit must ensure that the application will be compliant with the Outsourcing and Service Provider Access standard prior to going into production.
<input type="checkbox"/>	7. The application must be hardened and pass vulnerability assessments as described in the Vulnerability Management standard.



Related Documents

[Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems](#)

[Backup guideline](#)

[Development and Modification of Software Applications standard](#)

[Encryption Requirements standard](#)

[Internet-facing Systems and Services standard](#)

[Logging and Monitoring of UBC Systems standard](#)

[Outsourcing and Service Provider Access standard](#)

[Password and Passphrase Protection standard](#)

[Securing User Accounts standard](#)

[Transmission and Sharing of UBC Electronic Information](#)

[User Account Management standard](#)

[Vulnerability Management standard](#)