INFORMATION SECURITY CHECKLIST

Service Provider Security Risk Assessment Checklist

Introduction

1. This document is intended to assist Administrative Heads of Unit in managing their key privacy and security risks when engaging with a Service Provider.
2. This checklist has been issued by the Chief Information Officer to supplement the Outsourcing and Service Provider Access standard. Questions about this checklist may be referred to information.security@ubc.ca.
3. Administrative Heads of Unit who engage a Service Provider are responsible for ensuring the Service Provider is aware of the requirements in this checklist, and should use the checklist to validate the requirements are being met before, during, and after the Service Providers' engagement.

Checklist

☐	The agreement with the Service Provider will be signed by an authorized representative of UBC, such as Payment and Procurement Services.
☐	The Service Provider is aware of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems, and its accompanying standards.
☐	Prior to being granted access to High or Very High Risk Information, the Service Provider has signed a Security and Confidentiality Agreement (SACA) OR the primary contract with the Service Provider contains equivalent privacy and security language.
☐	The Service Provider's access to UBC Electronic Information and Systems is granted on the principle of 'least privilege', access is authenticated and role-based, and any access to UBC Systems containing High or Very High Risk Information is logged, where possible.
☐	Work of the Service Provider is monitored and reviewed by a UBC employee.
☐	The Service Provider stores UBC Electronic Information in a separate system or database, or has alternate controls.
☐	The Service Provider regularly backups UBC Electronic Information to a secure location in accordance with the terms and conditions as specified by the Information Steward/Owner.
☐	The Service Provider does not access or store Personal Information outside of Canada, unless legally authorized to do so.[1]
☐	The Service Provider transmits UBC Electronic Information in accordance with Information Security Standard #3, Transmission and Sharing of UBC Electronic Information.
☐	The Service Provider's access to UBC Electronic Information and Systems is revoked on completion of the project or termination of the agreement.
☐	Within seven days of project completion or termination of the agreement, the Service Provider: • returns all UBC assets in its possession to UBC, and • destroys UBC Electronic Information using destruction methods compliant with the Destruction of UBC Electronic Information standard, and provides a signed confirmation of destruction to the Administrative Head of Unit.

[1] *For example, temporary access or storage outside of Canada is allowed when necessary for installing, implementing, maintaining, repairing, trouble-shooting or upgrading an electronic system or recovering data from such a system; and is limited to the minimum amount of time necessary for that purpose.*

Related Documents

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems
Destruction of UBC Electronic Information standard
Outsourcing and Service Provider Access standard
Transmission and Sharing of UBC Electronic Information standard
Security and Confidentiality Agreement (SACA)