a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD U9
Outsourcing and Service Provider Management

1. Introduction

1.1 Service Providers (vendors, contractors, consultants and other non-UBC employees who provide services to UBC) may access, process, store or transmit UBC Electronic Information and Systems in order to deliver agreed-upon services. The increased security risk when access is extended outside of the organization needs to be managed appropriately. This standard is not intended to cover collaborations with other research institutions for research purposes.

1.2 This standard explains the information security requirements applicable to all Service Providers. The Administrative Head of Unit who engages a Service Provider is responsible for ensuring compliance with all of these requirements.

1.3 The Chief Information Officer has issued this standard 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. Security and Privacy Risk Assessment

2.1 Before Service Providers provision software applications or are granted access to UBC Electronic Information and Systems, information security risks must be assessed and managed using the Service Provider Security Checklist.

2.2 In addition to the requirement to use the above checklist, a Privacy Impact Assessment (PIA) is required if Personal Information is involved. Please refer to the PIA Process Overview for more information.

3. Cloud Service Providers

3.1 Cloud services providers (e.g. AWS, Azure) raise significant privacy and information security concerns as they store data outside of the custody of the University. Therefore it is essential to complete a PIA in each situation where these providers will be used.

4. Compliance with Policies and Standards

4.1 Before access is granted to UBC Electronic Information and Systems, the Service Provider must be made aware that it will be subject to Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems, and its accompanying standards.

5. Contractual Requirements

5.1 Service Providers must sign a Security and Confidentiality Agreement (SACA) prior to being granted access to Medium, High or Very High Risk Information. The Administrative Head of Unit may request the Office of the University Counsel to grant a waiver of the requirement for a SACA where the primary contract with the Service Provider contains equivalent privacy and security language. Doctors, lawyers, accountants, auditors, psychologists and other professionals who are bound by a duty of confidentiality do not need to sign a SACA.

6. Storage and Transmission of Information

6.1 Service Providers must store UBC Electronic Information in a logically separated environment, ensuring that the information is not mixed with information belonging to or accessed by other parties. If this is not possible, Service Providers may use alternative controls, with the written approval of the Administrative Head of Unit, to ensure that the data is secure and can be destroyed after the project is completed.

6.2 Service Providers must not access or store Personal Information outside Canada, as that would violate the BC *Freedom of Information and Protection of Privacy Act* (FIPPA) . It should be noted that UBC classifies Personal Information as High or Very High Risk Information. As an exception, temporary access or storage outside of Canada is allowed, provided that this is:

6.2.1 necessary for installing, implementing, maintaining, repairing, trouble-shooting or upgrading an electronic system or recovering data from such a system; and

6.2.2 limited to the minimum amount of time necessary for that purpose.

6.3 Service Providers must ensure that they transmit UBC Electronic Information in accordance with the Transmission and Sharing of UBC Electronic Information standard.

7. Access Controls

7.1 All Service Provider access to UBC Electronic Information and Systems must be granted as follows:

7.1.1 access must be authenticated and role based;

7.1.2 access must be granted on a Principle of Least Privilege (only the minimum level of access that is required to perform their duties); and

7.1.3 wherever possible, access to UBC Systems containing High or Very High Risk Information should be logged.

8. Ongoing Monitoring

8.1 The work of Service Providers must be monitored and reviewed to ensure that privacy, confidentiality and information security requirements are being satisfied.

9. End of Services and Data Destruction

9.1 Immediately upon completion of the project or termination of the agreement, whichever first occurs, the following must take place:

9.1.1 the Administrative Head of Unit must ensure that the Service Provider’s access to UBC Electronic Information and Systems is revoked; and

9.1.2 the Service Provider must stop accessing UBC Electronic Information and Systems.

9.2 Within seven days of the completion of the project or termination of the agreement, whichever first occurs, the following must take place:

9.2.1 the Service Provider must return all UBC assets (including access control cards and keys), equipment, and UBC Electronic Information in their possession; and

9.2.2 the Service Provider must destroy all UBC Electronic Information and hard copies of this information in its possession in compliance with the Destruction of UBC Electronic Information standard.

10. Related Documents and Resources

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

Service Provider Security Checklist

Privacy Impact Assessment (PIA)

Security and Confidentiality Agreement

BC Freedom of Information and Protection of Privacy Act (FIPPA)

Transmission and Sharing of Electronic Information standard

Destruction of UBC Electronic Information standard