The Province of British Columbia

Privacy Protection Measures

The measures listed in this document reflect a wide range of strategies available for consideration when negotiating a contract with a U.S. company or a Canadian company with a U.S. parent. There is no "one-size-fits-all" solution that is suitable for all contracts, and it is important to note that many of the measures listed here are being considered for large, long-term contracts that involve sensitive personal information. A thorough assessment of the specific project is required to determine what, if any, of the measures listed here should be incorporated into the contract.

September 2007

[redacted]

[redacted]	
1	[redacted]
1.1	Segregate personal information with restricted access.
1.2	Data and all back-ups only to be located in Canada.
1.3	Permit access to personal information only by personnel who require it in order to perform their duties.
1.4	Limit access to personal information through security measures (including passwords, IDs and similar measures) and restrictions on the issuance of passwords.
1.5	Adoption of privacy enhancing technologies over the term of the contract to improve security and restrict access to information to authorized users.
1.6	Physical security of data rooms and premises which house personal information with restricted access to authorized personnel only, high security for data rooms, servers and systems processors.
1.7	Audit and control procedures to ensure that measures effectively continue to limit access to personal information
1.8	Tracing and audit trails for data access, including access logs.
1.9	Regular audits including SysTrust audits.
1.10	To the extent reasonably possible, automatic notification processes, with notification to the Province, of access to personal information or data that is outside the ordinary course of business, including irregular or large scale access (e.g., unusual access patterns).
1.11	Restrictions on data mobility, including restricting data from leaving Canada in both physical and electronic formats (e.g. restrictions on outbound web and email access and hardware restrictions including limitations on floppy drives, CD ROM burners, USB smartdrives and similar devices). Note – location restrictions on carrying on business to apply throughout the term of the contract, including during a force majeure situation.
1.12	Detailed privacy and security standards in the contract including a requirement that Service Provider comply with the Province's security requirements (including the requirements of the *FOIPP Act* and other privacy legislation and the security requirements prescribed by the Office of the Chief Information Officer for the Province of BC and in chapter 12 of the Province's CORE Manual, including the Information Security Policy, version 1.1, March 2007, as updated.
1.13	Privacy policy covering issues such as data sharing, FOI requests and investigations consistent with provincial policy.
1.14	Security policies and standards including ISO17799:2000 (as revised from time to time).
1.15	Strong technology security measures including firewalls, encryption standards, authentication standards, and screen saver standards. Mandatory encryption of personal information on portable

	[redacted]
	storage devices including laptops. If for any reason the Service Provider does not comply, or anticipates that it will be unable to comply, the Service Provider must promptly notify the Province.
1.16	Adopt recommendations of the Commissioner, as found in the "Guidelines for Data Service Contracts", OIPC Guideline 01-02, as appropriate.
1.17	Province to complete a detailed Privacy Impact Assessment before contract is signed.
1.18	Risk and control reviews (including Privacy Impact Assessments) to be performed by Service Provider (to the satisfaction of the Province) prior to implementation of any material business or technology change.
1.19	Service Provider to sign an annual compliance certificate regarding security and privacy compliance.
1.20	Records and retention policies that conform to Province requirements.
1.21	Offsite storage for files should be in British Columbia, must be in Canada and should be approved by the Province with the Province having direct confidentiality agreement with the storage provider.
1.22	Security audit to be conducted prior to Service Provider's move into its permanent space.
2	[redacted]
2.1	Direct agreements between the Province and Service Provider employees. These agreements will include non-disclosure obligations and an obligation to advise the Province in the event that the employee becomes aware of any potential disclosure.
2.2	Direct agreements between the Province and all other people who are not Service Provider employees that have or could obtain access to personal information (including employees of subcontractors who are involved in the services and who would or could have or otherwise obtain access to personal information). These agreements will include non-disclosure obligations and an obligation to advise the Province in the event that the employee becomes aware of any potential disclosure.
2.3	Direct Agreements between the Province and the subcontractors that have or could obtain access to personal information which include applicable privacy and security obligations of the subcontractors to the Province, as well as non-disclosure obligations in respect of the personal information (including an obligation to advise the Province in the event that the subcontractor becomes aware of any potential disclosure).
2.4	Requirement that Service Provider include certain language in its employment agreements with its employees, including precedence of Province/employee direct agreement over the employment agreement and express agreement by Service Provider that there would not be adverse consequences to the employee for compliance with Province/employee agreement (whistleblower section).

	[redacted]
2.5	Service Provider must have an operational Privacy Plan (including protocol in the event of a security or privacy breach).
2.6	Appropriate training regarding the applicable processes and rules relating to access to and control of government information (e.g., what levels of access are permitted in respect of government information, including personal information, in what circumstances may such levels of access be varied, from which individuals may the employee receive instructions regarding such processes, and in what circumstances is the employee obligated to disclose to a supervisor (or the Province) the occurrence of activities that are inconsistent with the contract).
2.7	Annual re-training of employees and annual confirmation from employees that there has been no breach of Province/employee agreement.
2.8	Special security clearance requirements for employees who will have access to personal information.
2.9	Where reasonably possible, utilize employees of Canadian companies to do the work but when individuals that are employed by the U.S. company are used, ensure: (a) no data access unless absolutely required to perform duties; (b) "dummy" data be used to the extent possible so that people are not working on nor have access to "real data"; (c) if there is access, access would only be in British Columbia at the designated facility, with no ability to remove data from the premises, and each such employee must sign a direct agreement with the Province; and (d) data conversion would be overseen by (or monitored by) employees of the Province or Canadian companies that are subject to a Province/employee agreement.
2.10	If access to personal information must be permitted remotely from the US, then ensure: (a) there is written permission from the Province outlining the access; (b) it is consistent with FOIPPA; (c) it is limited, temporary and there is no storage of personal information ; and (d) no data access is permitted unless absolutely required to perform the services.
2.11	Whistleblower hotline to be set up for employees (including non-Service Provider employees) to report any potential disclosure.
2.12	Designated Canadian privacy, security and compliance officer responsible for monitoring and enforcing privacy and security measures.
2.13	Canadian employee as systems administrator.
3	[redacted]

	[redacted]
3.1	Detailed confidentiality and privacy provisions including a contractual agreement for Service Provider to comply with *FOIPPA* and *PIPA.*
3.2	Clear contractual provisions regarding Province ownership and control of the data (other than employment records which will be owned by Service Provider) with Service Provider custody of the data.
3.3	Requirement that Service Provider provide notice to the Province of any request from Service Provider's U.S. affiliates for government information including personal information (note that the confidentially requirements of the *Patriot Act* would not apply to a Canadian or B.C. company).
3.4	Express prohibition against access to personal information by a U.S. affiliate.
3.5	Province right to substantial liquidated damages from Service Provider in the event of any disclosure of personal information pursuant to a *Patriot Act* request (applies in the event of a disclosure made by Service Provider or any of its subcontractors).
3.6	The parent company is responsible for the upstream guarantee of the Service Provider obligations, including any liquidated damages as referenced in 3.5.
3.7	Termination rights in the event of any disclosure of personal information pursuant to a *Patriot Act* request (applies in the event of a disclosure made by Service Provider or any of its subcontractors).
3.8	Power of attorney in favour of the Province and other contractual rights that allow the Province to temporarily take over the operations of Service Provider to prevent a potential disclosure or to respond to an actual disclosure of personal information in connection with a *Patriot Act* request.
3.9	Trust structure to enable the Province to take over ownership of Service Provider if Province determines that there is an actual or potential disclosure of personal information to a foreign body.
3.10	Province to replace Service Provider employees with Province employees in order to prevent disclosure of personal information pursuant to a *Patriot Act* request.
3.11	Flow through of privacy and security provisions to subcontractors and affiliates of Service Provider, as specified throughout this privacy and security framework.
4	[redacted]
4.1	Subject to 2.9 and 2.10, all records containing personal information be in the sole custody of and may be accessed only by an entity incorporated in any province of Canada or pursuant to federal legislation.
4.2	All directors of Service Provider to be Canadian citizens and a majority of them to be British Columbia residents, each to sign a direct agreement with the Province restricting disclosure and requiring the director to advise the Province of any potential disclosure of personal information.

	[redacted]
4.3	Restrictions in the incorporation documents of Service Provider that make disclosure, of personal information contrary to Canadian and British Columbia law, outside of the company's corporate authority.
4.4	Three layer corporate structure with Service Provider being wholly owned by a Canadian entity who, in turn, is owned by the U.S. company, thereby removing direct ownership of the Canadian Service Provider by the U.S. parent company.
4.5	Requirement that subcontractors be Canadian controlled entities. Any change in such control without Province consent can be grounds for terminating the contract if the subcontractor is to continue providing the services.
4.6	Assignment of contract and change of control of Service Provider without Province consent is an event of termination.
4.7	Disclosure of personal information by Service Provider or any of its subcontractors (who could or would have access to personal information), other than in the ordinary course of performing the services, will be subject to approval of Service Provider's Canadian chief legal counsel who is a member in good standing of a Canadian bar. Chief legal counsel to advise the Province in writing of any requests for such disclosure, prior to the disclosure being made.