Canadian Pacific

(Third Party)
Security Assessment
(Questionnaire)

For

<Project/System Name>

Enterprise Security

Version Updated: February 2015
Version 2.01

Table of Contents

Purpose

This purpose of this questionnaire is to establish a baseline security understanding of the proposed <project/system name> for use by CP. This document would be used to 1) determine whether the proposed application adheres to current CP policies and procedures; 2) document industry security best practices; and 3) to certify that the application is safe and secure and for use within CP environment.

As this is a high level questionnaire, additional information may be sought to further clarify potential areas of risk or exposure.

For the purposes of this document, the following terms are used:

- "Vendor" refers to **<supplier/provider/vendor name>**.
- "System" or "Systems" refer to any and all Vendor systems (servers, workstations or network devices) on which CP data will be stored, processed, manipulated, or transmitted.
- "Data" refers to any CP data, in original format provided by CP, or in any data format created by the Vendor in order to store, process, manipulate, or transmit the data.

1. General Information Security

1) Application, System or Project Name

Vendor Comments:

2) Will Data be processed or retained outside of Canada?

Vendor Comments:

3) Will Data be processed or retained by a third party other than Vendor?

Vendor Comments:

4) Has the hosting site undergone evaluation/certification by a third party security company (PCI, SOX, SSAE16, etc.)? What is the frequency of these audits? Can Customer obtain copies of the audit reports upon request?

Vendor Comments:

5) Will Vendor allow Customer to conduct site surveys of Vendor hosting site and review Vendor's physical and information security processes and controls, including independent security assessment?

Vendor Comments:

6) Will Vendor notify Customer in writing within 24 hours of any incident that compromises, corrupts, or destroys Data or Systems?

Vendor Comments:

2. Security Architecture

1) Provide a high-level architecture diagram showing all System components (including protocols, middleware, etc) required for this application.

Vendor Comments:

2) Describe OS, application, and database software (including versions and release levels) installed on each server in the hosting infrastructure.

Vendor Comments:

3) If the infrastructure hosting Data will be physically separated and physically secured from other customers' equipment and data, please describe how this will be accomplished. If not, describe how Data will be protected from the possibility of "horizontal" attacks on one customer from another.

Vendor Comments:

4) Are there access controls in place to determine who can access/manage the datacenter infrastructure, applications, databases and/or servers? Are access controls defined by: User group? IP Addresses/networks? Protocols?

Vendor Comments:

5) In the event of a security incident, how will Vendor disable all or part of the infrastructure containing Systems or Data?

Vendor Comments:

3. Network Security

1) Describe network and security components in the hosting infrastructure (firewalls, IDS/IPS, routers, switches, etc.).

Vendor Comments:

2) Describe the process for updating/patching the infrastructure components. Who is responsible for identifying new vulnerabilities in firewalls, IDS, network devices?

Vendor Comments:

3) Are vulnerability scans and penetration tests performed on the network and application hosting infrastructure? What is the frequency of these tests and who performs them? Can Customer obtain copies of the testing reports upon request?

Vendor Comments

4) Are the Firewall and network device logs monitored for anomalies on a 24x365 basis? What are the trigger points for a security event?

Vendor Comments:

5) Does the infrastructure include an Intrusion Detection System (IDS) consisting of both host-based and network-based sensors? Are the sensors monitored on a 24x365 basis for anomalies? What are the trigger points for an IDS event?

Vendor Comments:

6) Are the network device logs analyzed daily for anomalies? Are network logs retained for at least 6 months?

Vendor Comments:

7) Are the firewall, IDS and network device logs synchronized to a common time source and common standard (i.e. GMT)?

Vendor Comments:

4. Server Security

1) Explain how Systems, including operating systems, applications, databases, etc., have been "hardened" against attacks.

Vendor Comments:

2) Describe the process for updating/patching System OSes, applications and databases. Who is responsible for identifying new OS, application, database vulnerabilities? How long does it take to patch for: Critical patches? High patches? Moderate patches?

Vendor Comments:

3) Are vulnerability scans conducted on Systems, including servers, applications and/or databases? How often are they scanned? What is the process for remediating vulnerabilities discovered during scanning?

Vendor Comments:

4) Are security tools installed on servers to detect viruses, malware, spybot and other Trojan software? How often are these tools updated?

Vendor Comments:

5) Do you:
   - ❑ Have documented information security baselines for every component of your infrastructure (ex. Hypervisors, operating systems, routers, DNS servers, etc?)
   - ❑ Have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?
   - ❑ Allow your clients to provide their own "trusted" virtual machine image to ensure conformance to their own internal standards?

Vendor Comments:

6) Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?

Vendor Comments:

7) Do you have a capability to detect attacks which target the virtual infrastructure directly (ex. shimming, Blue Pill, Hyper jumping, etc.)?

Vendor Comments:

5. Application Security

1) What types of privileges are required to run the application? Does the application need to run under the “administrator”, “root”, “superuser”, “local services”, etc., accounts?

Vendor Comments:

2) Please describe the web application security process, if applicable.

Comments:

3) Does the application use symmetric or asymmetric cryptography? If so, explain encryption algorithm(s), key length(s) and where it is used.

Vendor Comments:

4) If the application stores or transmits Data containing passwords, Personally Identifiable Information (PII), or company sensitive/proprietary information, does the application support end-to-end document encryption? Explain encryption algorithm and key length.

Vendor Comments:

5) Does the application provide the ability to encrypt Data at the field or database level? Explain encryption algorithm and key length.

Vendor Comments:

6) Are code reviews performed on the application on a regular basis for the explicit purposes of finding and remediating security vulnerabilities? If so, who did the review, what were the results, and what remediation activity has taken place?

Vendor Comments:

7) Describe the quality assurance process for detecting common security issues such as cross-site scripting, buffer overflow, SQL injection, invalidated input, etc. within the application.

Vendor Comments:.

6. Data Protection

1) Does Vendor have policies and procedures in place for the handling and protection of personal information, including a company privacy policy? If yes, are these policies and procedures readily available to internal personnel and third parties who wish to review them?

Vendor Comments:

2) Are secure electronic transmission channels (minimum128 bit) utilized for all electronic transmissions of Data between Customer and Vendor, or any time Data could be intercepted during transmission?

Vendor Comments:

3) Is authentication to specific user accounts on both source and destination systems required prior to electronic transmission of Data (e.g., no “anonymous” or “guest” accounts)? Is the authentication process encrypted (e.g., not in clear text)?

Vendor Comments:

4) Describe Vendor’s procedures for the storage, reuse, and disposal of physical media (disks, tapes, removable media, etc).

Vendor Comments:

5) Do you have the ability to logically segment, encrypt and recover data for a specific customer/tenant in case of a failure, data loss or in the event of legal demand, without inadvertently accessing another tenant's data?

Vendor Comments:

6) Does your system support or have:
   - ❑ Structured data-labeling standard?
   - ❑ Capability to identify virtual machines via policy tags/metadata?
   - ❑ Capability to identify hardware via policy tags/metadata/hardware tags?
   - ❑ Capability to use system geographic location as an authentication factor?

Vendor Comments:

7) Do you allow tenants to define acceptable geographical locations for data location and routing or resource instantiation? Please explain.

Vendor Comments:

8) Do you have?
   - ❑ Data leakage and data loss prevention system?
   - ❑ A process/ technology to protect customer/tenant against data mining?
   - ❑ Technical control capabilities to enforce tenant data retention and disposal policies?
   - ❑ Documented procedure for responding to requests for tenant data from governments or third parties?

Vendor Comments:

9) Do you have an identity management system in place which enables both role-based and context-based entitlement to data?
   - ❍ Yes
   - ❍ No

Vendor Comments:

7. Business Continuity / Disaster Recovery

1) Describe Vendor business continuity/disaster recovery processes.

Vendor Comments:

2) Describe the data backup process. How often are backups performed? Is tape encryption utilized? What is the time period before a tape is rewritten or rotated?

Vendor Comments:

8. Authentication, Authorization and Access Control

1) Describe your password policies:

   a) How often are users prompted to change passwords?

   b) What are the password requirements?

   c) How are passwords encrypted?

Vendor Comments:

2) Describe the application user account characteristics and process.

Vendor Comments:

3) When certificates are utilized for Customer authentication, does the application store the certificates securely and protect them appropriately?

Vendor Comments:

4) Does the application have clear mechanisms for the granting, revocation, and suspension of certificates? The certificates should be checked every time they are presented.

Vendor Comments:

5) Does the application provide role-based authorization enforcement capabilities?

Vendor Comments:

6) What is the process and associated responsibilities for the approval of new userids/access and the removal of access that is no longer required?

Vendor Comments:

7) Does the vendor require (or offer) periodic re-approval and/or synchronization of userids with our internal identity management solutions? If not, how does the vendor ensure that only authorized people can access the application?

Vendor Comments:

8) Does the application restrict access control on a need-to-know basis?

Vendor Comments:

9) Does the system prohibit software uploads or configuration changes to the operating system by anyone other than an authorized administrator?

Vendor Comments:

9. Application Audit Trails

1) Does the application create log and audit trails containing at a minimum the User ID and timestamp for critical and security related activities and processes? Please provide detail.

Vendor Comments:

2) Are the server, application and database logs analyzed daily for anomalies?

Vendor Comments:

3) Does the application provide a means for audit trails to be archived via a definable time cycle?

Vendor Comments:

4) Are logs synchronized to a common time source and common standard (i.e. GMT)?

Vendor Comments:

10. Physical Security

1) Describe the physical security within the hosting site and the equipment hosting Data including: access control procedures (proximity cards, cipher locks, biometrics, etc), access hours, alarm and monitoring systems (cameras, guards, etc.).

Vendor Comments:

2) Explain the procedures for reviewing physical access controls (logs, video tapes, etc) and the archival process of such data (how often, where are archives kept, retention period).

Vendor Comments:

3) Describe Data Centre environment (provide sufficient detail to understand quality of environment - power, uninterrupted power supply, security, access, staffing, hardware, cabling, network, raised floors, HVAC, fire detection and suppression systems etc.)

Vendor Comments:

11.Responsibilities

1) Do you provide tenants with a role definition document clarifying your administrative responsibilities vs. those of the tenant? Please provide documentation.

Vendor Comments:

2) Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents? Please provide documentation

Vendor Comments:

3) Do your organization's service level agreements provide tenant remuneration for losses they may incur due to outages or losses experienced within your infrastructure?

Vendor Comments:

4) Do you provide tenants with documentation showing the transport route of their data between your systems? Please provide documentation.

Vendor Comments:

12.Attestation

To the best of my knowledge, the answers to these questions accurately reflects the security and risk management policies, practices and technologies in place on the date indicated below

Signed:	
Name:	
Title	
Company	
Date	