PIPEDA / PIPA Compliance Policy

Last Update Status: Updated August 20, 2015

1. Overview

TRINUS Technologies Inc. (TRINUS) intentions for publishing a *PIPEDA / PIPA Compliance Policy* is to ensure that all employees, contractors, partners, clients, and customers are aware that TRINUS considers information privacy and IT Security to be a high priority. TRINUS has prepared several individual policies which shall address overlapping information protection and security issues. This policy and selected affiliate policies will be available electronically for public consumption.

2. Purpose

The purpose of this policy is to highlight overarching concepts and best practices associated to personal information protection.

3. Scope

Information and personal security risks and mitigation strategies are not limited to cyber security. TRINUS has also imposed physical security layers, in order to enforce strict access to information permissions and protocols. The following policies and procedures should be cross-referenced when researching TRINUS procedures related to personal information protection:

a. Acceptable Use Policy
b. Email & Fax Policy
c. Records Management & Information Security Policy (Risk Management)
d. Human Resources Information Security Policy
e. IT Incident Management Policy
f. IT Infrastructure Security Policy

4. Policy

4.1 Physical Security

4.1.1 TRINUS shall implement reasonable physical security measures, in order to increase the level of protection of personal and corporate proprietary information / data. These include but are not limited to the following:

4.1.1.1 The completion of physical security assessments.
4.1.1.2 Perimeter re-enforced doors, windows, and locks.
4.1.1.3 Alarm systems.
4.1.1.4 Video surveillance systems.
4.1.1.5 Visitor access controls.
4.1.1.6 Locked cabinets.
4.1.1.7 Restricted areas.
4.1.1.8 Protection of client / customer keys, access cards, alarm codes and passwords. (See Appendix "A")

4.2 Workstation Security

4.2.1 All employees, contractors, consultants, and partners of TRINUS that have access to personal information and/or the TRINUS internal network, must take appropriate measures to protect their workspace from unauthorized access. Consequently, the following "clean desk" practices shall be enforced:

4.2.1.1 Computer or electronic devices that have access to the TRINUS network shall be password-encrypted with an additional password-protected screen saver activated after 3-10 minutes maximum, depending on the classification of the data (ie: A, B, C, or Confidential).
4.2.1.2 Computer or electronic devices that have access to the TRINUS network shall not be left unattended, unless logged out or locked.
4.2.1.3 Hard copy information classified as Protected C shall be locked in a drawer or cabinet.
4.2.1.4 Media storage containing information classified as Protected C shall be locked in a drawer or cabinet.

4.3 After Hours / Closing Protocol

4.3.1 In order to ensure no personal information of data is left exposed for public consumption or loss after the work areas are left unattended, the following "closing" protocol shall be implemented. The last person to leave the work area shall:

4.3.1.1 Inspect all work surfaces for loose documents or electronic media.
4.3.1.2 Inspect all computer workstations.
4.3.1.3 Inspect all printers and fax machines.
4.3.1.4 Inspect all *Point of Sale* devices.
4.3.1.5 Inspect all mail boxes.
4.3.1.6 Inspect all locked cabinets and/or office doors.
4.3.1.7 Lock computer server rack doors.
4.3.1.8 Lock computer server room access.
4.3.1.9 Close window blinds.
4.3.1.10 Check for unauthorized personnel.
4.3.1.11 Check that all external windows and doors are locked.
4.3.1.12 Activate the intrusion alarm system(s).

4.4 Data Security

4.4.1 TRINUS shall implement *reasonable physical security safeguards* and compliance procedures for the protection of electronic data, in order to increase the protection level of personal and corporate proprietary information / data. These include but are not limited to the following:

4.4.1.1 Secure server rooms.
4.4.1.2 Data loss prevention plans.
4.4.1.3 IT threat countermeasures.
4.4.1.4 Email activity audits.
4.4.1.5 Network attack audits.
4.4.1.6 Software inventory.
4.4.1.7 Hardware inventory.
4.4.1.8 Storage media inventory.
4.4.1.9 BYOD approval procedures.

4.5 Privacy Information Breaches

4.5.1 In the event of privacy information breach, either as a result of a network attack or physical security failure, the Director of the *IT Security Department* of TRINUS shall investigate. All breaches or privacy information losses shall be reported to the Privacy Commissioner of Alberta, in accordance with the *Personal Information Protection Act (PIPA).*

4.6 Business Continuity

4.6.1 TRINUS shall document a *Business Continuity Plan* (BCP), which may incorporate *Data Loss Prevention Plans* (DLPP) and *Disaster Recovery Plan* (DRP). The BCP will consider the following issues among others, as articulated in the plan:

4.6.1.1 Backup procedures, on and off site.
4.6.1.2 Backup restoration testing.
4.6.1.3 Levels of service interruption.
4.6.1.4 Physical damage.
4.6.1.5 Environmental damage.
4.6.1.6 Unauthorized modification or disclosure of information.
4.6.1.7 Loss of control of system integrity.
4.6.1.8 Physical theft.

5. Policy Compliance

5.1 Compliance Measurement

The TRINUS team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the TRINUS team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

a. Acceptable Use Policy
b. Email & Fax Policy
c. Records Management & Information Security Policy (Risk Management)
d. Human Resources Information Security Policy
e. IT Infrastructure Security Policy

7. Definitions

None specific.