ABC Information Security Policy

Jordan Ell, *University of Victoria*

Subject Area

Laptops are personal computers given to ABC employees in order to assist face paces business process and increase productivity. These laptops can be used both at work and home to allow employee connectivity to work at all hours. These laptops can contain all manor of information regarding ABC, its employees, and customers. Laptops have become a high risk data loss item because of an increase of malicious software / hardware sophistication as well as a decrease in these malicious intents cost.

The loss of an ABC issued laptop not only incurs the physical cost of laptop replacement, but is also subject to data security issues. These data security issues are also present in unattended laptops as well as stolen. It is important that ABC personnel become aware of the potential security risks involved in laptop use and take all possible steps to ensure laptop and data security of their machine. This policy offers guidance on the user of ABC issued laptops in both their physical protection as well as virtual.

Areas of Concern

The primary area of concern is the loss of confidential company information regarding the company itself, employees, or customers. These losses can be brought on by irresponsibility of laptop ownership which can lead to laptop theft and potential data theft of the laptop's contents. With newly emerging quick and relatively cheap forms of data theft such as cold boot attacks, laptop information security has become a primary concern of ABC. Factors of laptop use which can lead to these attacks and data loss include:

- Laptop theft.
- Unattended powered on laptops.
- Sensitive data being stored on personal laptops.
- Low refresh rates if DRAM.
- Unprotected laptop BIOS.
- Laptops being left on for extended periods of time.
- Hard drive being unencrypted.
- Data loss of unsecured laptops and hard drives.
- DRAM attacks such as cold boot attacks.
- Company wide security breaches due to a single laptop being attacked.

Intended Outcome

This policy for information security is intended to prevent virtual and physical loss to the company in the following ways. First, to prevent physical laptop theft. Second, to prevent data loss attacks on laptops which need not be stolen or moved from their location. Finally, to promote responsible laptop use and ownership among all employees of ABC.

Information Security Policy

The policy outlined here is broken into responsibilities of different types of personal with a bottom up approach. An employee who falls under any of the

listed categories must strictly adhere to the rules outlined.

Responsibilities of all Personnel

Technical

- Ensure a BIOS password is installed on ABC issued laptop.
- Ensure no company sensitive data is stored on issued laptop. This includes company, employee and customer related sensitive information.
- Ensure hard driver encryption is installed and used on ABC issued laptop.

Physical

- Ensure laptop is locked to immovable object when available.
- When laptop is to be left unattended for longer than 10 minutes, the laptop must either be locked in a cabinet or other secure location or must be powered off while be locked to an immovable object.
- When laptop is not being used to an extended period of time (at the end of the work day or other), the laptop must be powered off.

Avoid

- Leaving laptop powered on for extended periods of time even in a secure location.
- Giving laptop to any ABC employee other than IT for an extended period of time.

Report

- Any laptop seen unattended and not securely fasten with laptop lock or secured inside locked cabinet.
- Any discrepancy with technical measure such as BIOS password, secure data storage, or hard drive encryption.
- Any actual and suspected security incidents involving physical or data loss.

Responsibilities of IT

Technical

- Ensure only high refresh rate DRAM is purchased and installed on any ABC laptop issues to employees.
- Ensure any hard drive encryption also flushes DRAM when the laptop is powered off.
- Ensure proper training in all technical controls are issued to new employees of ABC and that compliance metrics are met.

Compliance

- Ensure data security information sessions are held with each department of ABC are held at least once a year to update employees about new security measures and concerns.
- At the department's discretion, perform spot checks of departments or employees laptops to ensure policy standards are being met.
- Ensure employees properly patch software as needed on laptops as patching requires employee presence with BIOS password.

Avoid

- Sensitive data being stored on internet facing servers or ensure proper security measure have been taken for data security.

Responsibilities of HR

Physical

- Ensure all new employees are trained on proper laptop security. This includes all physical items listed in the responsibilities of all personnel.

Compliance

- At the department's discretion, perform spot checks of departments or employees laptops to ensure physical policy standards are being met.