ABC CORPORATION
Policy No. 1
Laptop Security
Information Security Branch
Office of the Chief Information Officer
ABC Corp

http://www.abccorp.com

1 SUBJECT AREA DESCRIPTION

Laptops are in use across ABC corporation. They are used for portable computing and providing a method for productivity while out of the office. Laptops are intended for business use only. Laptops have different ports on them including USB, CD-ROM drives, SD-card readers, and more. These laptops can have sensitive business data on them when employees are using them for work, and this data can include: customer information, business reports, analyitics, inside information, proposals, and more. When dealing with such sensitive information, the laptops need to have their information protected.

ABC corp has very sensitive information on the laptops, and it is very important that each employee knows about the dangers of leaving their laptops unattended or unlocked. Although ABC uses advanced methods of keeping the data on hard drives encrypted and safe, keeping these laptops secure is of utmost importance. The realization of a threat of a compromised ABC laptop would have cause irreparable damage to ABC. This policy addresses security concerns regarding compromised ABC laptops and offers guidanace and standards for employees to protect their asset, and ABC.

2 AREAS OF CONCERN

The most important asset is not the laptop itself, but the information on it. ABC is concerned with the control of sensitive information on company laptops, and with new methods of attack for data theft, ABC has identified these some primary concerns with technical and physical use of ABC laptops:

- Unattended Laptops in sleep mode or powered on
- Encryption keys for hard disk security stored in DRAM
- Stolen ABC laptops
- DRAM with low refresh rates
- Unnecessary sensitive data stored on company laptops
- Cold boot attacks[1]
- Unencrypted sensitive data
- Bad data separation, causing one compromised laptop to give access to many assets in the company

[1] Attacks that are used by stealing the contents of RAM, containing the encryption key, then gaining access to the encrypted hard disk. http://en.wikipedia.org/wiki/Cold_boot_attack

3 INTENDED OUTCOME

The policies around ABC corp. laptops are intended to:

- Reduce the risk of a cold boot attack succeeding
- Improve awareness among ABC employees about the importance the welfare of sensitive data on their laptops
- Decrease the amount of stolen ABC laptops
- Educate ABC employees about deleting data when unneeded
- Improve knowledge of safe Laptop transport and storage
- Reduce the risk of a compromised laptop, and reduce the amount of damage a stolen laptop would incur.

4 *Responsibilities of all Personnel*

Things to do

- Never leave a laptop unattended without tethering it to a secure object with the given cable locks.
- Only leave your laptop unattended at the office, or another safe location.
- Whenever left for more than 20 minutes, ensure that the laptop is powered down.
- Ensure that sensitive data is used only when absolutely necessary, and when it is used it is deleted securely after it is no longer needed.
- Use the encryption key FOB[2] given to you by the IT department, and ensure it is always with you.

Things to avoid

- Use the ABC laptop for personal use
- Store sensitive data on the laptop for long periods of time
- Leaving an encryption FOB with a laptop

Things to report

- Other employees not adhering to the security standards
- Potential attempts at stealing laptops
- File a incident report immediately after a laptop is missing

5 *Responisibilities of IT Personnel*

Things to do

- Install Encrypytion key FOBS and issue them to all employees at ABC.
- Seal the DRAM with a physical lock onto the motherboard to prevent attackers from physically stealing the DRAM
- Disable booting from any media other than the encrypted hard disk by changing BIOS settings.

Things to avoid

- Improperly installing any of the security features described in the policy.
- Moving sensitive data from any of the laptops, or storing any sensitive information on an unsecure medium

[2] A small device that uses rolling codes to enable encryption on the hard disk by a proximity to the device

6 COMPLIANCE

In order to have universal compliance of the policy, all aspects of the company must be involved in the compliance techniques. Over a period of 3 months, there will be standardized security refreshers among the staff.

Responsibilities for HR

- Organize the meetings for employees to get security refreshers from the IT department.
- Advertise the importance of laptop security around the office with posters, emails, and meeting sessions.
- Perform routine checks of the office by checking for unattended laptops and misuse of security technology

Responsibilities for IT

- Perform routine checks on the health of the physical security measures in place.
- Ensure that the laptop cannot boot from any other media than the encrypted hard disk
- Ensure that the FOB is working correctly
- Ensure that proper training is given to all ABC employees regarding the security policies