SOFTECTION

An Effective Corporate Laptop Security Policy

SOFTECTION
DIGITAL ASSET PROTECTION

An Effective Corporate Laptop Security Policy

www.softection.com

Executive Summary

Corporate laptops are often the biggest data security threat for a company. Laptops contain highly sensitive information, but are extremely vulnerable to theft or loss. Still, 73% of companies do not have security policies specifically relating to laptops.

This White Paper outlines an effective laptop security policy based on best practices gained from a range of clients and industry experts. It was developed for the benefit of companies looking for heightened laptop security, and designed with the idea that good policies must have three traits:

1. They must be enforceable.
2. They must provide accountability.
3. They must be auditable/measurable.

If you are in the process of developing a laptop security policy for your company you can use the outline below as a foundation.

Corporate Laptop Security Policy

Theft Prevention

- Provide employees with theft prevention training. This will take only minutes for users to complete, and should include information on:
  - Keeping laptops out of sight when not in use.
  - Not leaving laptops on the car seat of a parked car.
  - Carrying laptops in something other than a laptop bag to avoid an obvious target.
  - Keeping laptops locked to something secure, even while in the office.
  - Special information for travelers on things to watch out for in airports, taxis, hotels, conference rooms, and other places they are likely to visit.
  - Other policy information.
- Enforce laptop locking. Many laptop thefts occur on site so physically securing laptops even within the office can prevent theft:
  - This is more difficult to enforce for traveling employees and there are still times in transit where laptops will be vulnerable to theft, but the benefits of securing machines within an office make this worthwhile.
- Implement other physical security policies, including, but not limited to:
  - Restrict physical access to different areas of office.
  - Ensure visitors are always accompanied.
  - Consider attaching transponders to laptops which can be used to track entries/exits from the building.
  - Consider installing cameras at exits.
- Attach ID tags to laptops (a business card would work, but tamper proof tags are preferred). These tags must have a contact number and a simple way to identify the laptop. Many laptops are accidentally left behind and are found by somebody who would return it if there was an easy way to get in touch with the owner.
- Provide adequate secure storage for laptops on the premises for after-hours locking up.
- Some companies prefer to have employees purchase there own laptops or sign responsibility agreements with the idea that it will result in more caution being taken. There are no published studies on the success of this, but it is worth your consideration.

SOFTECTION
DIGITAL ASSET PROTECTION

An Effective Corporate Laptop Security Policy

www.softection.com

Hardware Recovery

- Record all serial numbers of laptops, and register with the manufacturer and supplier. Also register the serial numbers with the police when a theft has occurred:
  - If a laptop is stolen and is later brought in for servicing it can be identified as stolen if this step is taken.
- Install laptop tracking software that will trace the location of a laptop that has been stolen:
  - According to the FBI, 97% of stolen laptops are never recovered. Smart criminals will know how to bypass this software easily, but these solutions tend to be low cost.

Limiting the Risk of Stolen Data

- Implement a secure password policy to make it very difficult for a thief to log on to a stolen laptop:
  - Prevent usernames from being remembered on the login screen.
  - Force password changes on a regular basis.
  - Ensure passwords contain upper and lower case characters and numbers.
- Encrypt important data:
  - All important data within an organisation should be encrypted, not just that on a laptop.
  - Encrypting only important data is preferred as entire hard drive encryption does have a noticeable affect on performance.
- Keep an up-to-date backup of all data to ensure that work isn't lost if a laptop goes missing.
- Set time-bombs on important data:
  - If a laptop has not been connected to the network for some set period of time, important data on it should be wiped.
- Centrally administer access to data:
  - Prevent certain types of data from being accessed on unconnected laptops. Without a scheme to centrally administer and enforce this, it is highly likely that this data will end up on laptops in unprotected form.

Conclusion

By instituting these policies, customized to your specific needs, you will be able to reduce the risk of hardware theft, and limit the risk of stolen data if/when a theft occurs.

Softection's products offer solutions ideal for data protection on laptops and can help you meet the demands for protecting your confidential data. The range of products also extends beyond laptop protection to full data management and security solutions. Please contact Softection for more information on how we can help you keep your data safe.

Web: www.softection.com
Email: laptops@softection.com
Phone: +61 2 9816 3433

SOFTECTION
DIGITAL ASSET PROTECTION