"YOUR LAPTOP, YOUR RESPONSIBILITIES"

A Suggested Physical Laptop Security Policy for Private and Public Organisations by Kensington and IDC

Introduction

This document serves to outline The Company's policy on the use and storage of your laptop. This is intended to minimise The Company's exposure to information security risk as well as increase the user's personal safety and safeguard the company's hardware investment.

Portable computing equipment is not just stolen to be resold, it is also stolen for the information it contains. Information about customers, employees and payments, and commercially sensitive data can all be of value to a thief. In the wrong hands, the information on your PC equipment could be a risk to The Company.

The Company relies heavily on its ability to access up-to-date and complete business information; the loss or unauthorised modification of data on portable devices can impact heavily on the company's ability to trade effectively or management's ability to make informed business decisions. So, the cost to the business can persist long after the initial security breach and be of far greater consequence than hardware value alone.

- The average small company loses 4 laptops a year to theft*
- Only 7% of stolen laptops are recovered*
- The true cost to business of lost or stolen laptops is more than three times the cost of the hardware*
- The security of customer/client information is the primary concern when laptops are stolen*

Physical Security — Laptop Policy

Employees will be provided with a laptop when it is essential to their productivity and function. When issued with a company laptop, users accept to abide to, and champion, the company's physical laptop security policy.

- It is company policy to issue every laptop user with a T-bar lock.
- Users who require additional locks for other portable equipment should inform the helpdesk or ask their line manager.
- In recognition of the increased convenience and likelihood of better policy compliance, it is company policy to offer a second lock for regular travellers. It is the responsibility of the employee to contact their line manager and the helpdesk should they travel regularly.
- If a lock is missing, the employee should inform the helpdesk.
- Where locks are issued, users are expected to:
  - Lock equipment at all times in areas open to the public, even when in use.
  - Lock equipment while travelling whenever possible.
  - Lock equipment at home when not in use.

IDC EMEA, 389 Chiswick High Road, London, W4 4AE, U.K. Tel.+44.20.8987.7100 www.idc.com

Physical Security — Laptop Policy Enforcement

- In recognition that a lock only reduces the risk of laptop theft, the company expects all line managers and the helpdesk to reinforce the need for users to be aware of the risk of theft and to offer advice including the following:
  - Don't depend on a lock as the only security.
  - Always lock out of sight if not in use.
  - Never leave a laptop logged on to networks, email and Web sites. Always shut down or activate a password-protected screensaver.
- It is company policy to demonstrate how physical security locks should be used at first issue to users. The company will reinforce this message no less than once annually.
- It is company policy to support further training for the use of physical security locks if requested.

Appropriate Use — Laptop Policy

- The Company does not tolerate inappropriate use of any company property. Use your laptop only for business purposes. Offensive, pornographic, racist or abusive content found on company laptops will be referred as necessary under The Company's disciplinary proceedings. Serious offences will be reported as necessary to the police.
- Your email should be filtered for spam. If you receive any inappropriate material by email delete it immediately. If persistent, report to the helpdesk for investigation.
- Only visit Web sites you know and trust.
- The company network is monitored for inappropriate use. Offenders will be reported to their line managers for further disciplinary action.

The Company's Laptop User General Responsibilities

General

- Don't leave laptops unattended and always lock.
- Don't allow anyone else to use your laptop — it is company equipment and provides access to our networks.
- If left at work overnight, lock out of sight.
- Choose an ordinary looking briefcase or non-traditional laptop carry bag, perhaps a backpack type, as bags that obviously contain computers are an easily identifiable target for the casual thief.

At Home

- Always store inside your home, never leave in the car and keep where it cannot be easily seen from outside. Ideally, keep locked in a cupboard or strong drawer.
- When it is not possible to lock away, use your supplied T-bar lock attaching to either an immoveable object or to something that is difficult or heavy to carry.
- Do not allow any use that is not authorised by The Company.
- Only use in an office-like environment with table and chair. Do not be tempted to use near water.
- Only connect to approved or known wireless networks. Ideally use your encrypted domestic connection if available.

In the Car

- Your laptop will be safer if it is not left in the car at all.
- If absolutely necessary, lock out of sight in the boot.
- If you expect to leave your laptop in the car regularly, speak to the helpdesk and ask about additional security measures. An in-car vault or separate lock to leave in your boot which can be locked to the spare wheel may be offered.
- Consider the overall security of the vehicle in terms of the location, time of day and duration of your stay when parking.
- While the vehicle is in motion, your laptop should be stored in its carry bag. Ideally secure in the boot; a heavy item such as a laptop can become a hazard to vehicle occupants in an accident.
- Only connect to approved or known wireless networks.

Public Transport and Public Places.

- Laptops are particularly vulnerable to theft and loss while using public transport. Be vigilant.
- Do not use your laptop while travelling unless necessary. Even then, consider the location you choose with care. Ensure you are not easily overlooked and never open documents or communications that are of a commercially or personally sensitive nature while in a public place.
- Never leave unattended and never allow anyone else to use your laptop.
- Be aware of your surroundings. Ensure you are not exposing yourself or the laptop to opportunistic theft.
- Always use your T-bar cable lock, even when working, to avoid the laptop being easily snatched.
- Only connect to approved or known wireless networks.

Hotels, Conference and Meeting Rooms

- Avoid leaving laptops in hotel rooms. Use the hotel safe and get a receipt. If absolutely necessary, use your T-bar lock.
- In conference and meeting rooms, use your T-bar lock. It is good practice to do this even when working so that it isn't later forgotten at a coffee break. For longer breaks, shut down and take your laptop with you.

The Company's Laptop User Data Protection Responsibilities

- Always use encryption software approved and supplied by The Company.
- Choose a password that is unique to your data-encryption key; make it long, random and complicated to guess.
- Do not give your network password or token/access device to anyone. You are responsible for all access under these codes.
- Remember that access to your laptop can also mean access to The Company's network.
- Your laptop is the property of The Company; do not lend it to anyone or otherwise permit use by anyone else, not even for a short while.
- If you leave your laptop switched on and unattended you must activate the password-protected screensaver. Ideally, never leave switched on or logged in. Log out, shut down.

The Company's Laptop User Malware Responsibilities

- Malware is harmful software such as viruses and spyware. Malware on your laptop could be spread to the wider company network or risk the security of the data on your laptop. It is important that no malware should be allowed on your computer.
- The Company provides all laptop users with pre-installed antivirus software. Make sure you know how to access and use this software. Call the helpdesk for advice if needed.
- If you do not have regular access to The Company's network then you will not receive regular antivirus updates. Make sure you log on to the company network at least once a week to allow for these important updates to take place. If this is not possible, talk to the helpdesk about ways to keep your antivirus application definitions current.
- Always scan files for viruses. Your email is automatically scanned for you as are files from the company network, but if you are given a file on a disk, USB key or by any other means then you must first scan the disk and/or file for viruses.
- Do not open any email attachments unless they were expected and from a trusted source. Email attachments are the number-one malware risk.
- Do not download any software. If you need a different or more current application, contact the helpdesk for advice. Most permitted applications are updated automatically for you when you log into the company network.
- If you suspect a virus attack, contact the helpdesk immediately. Do not access the company network or back up files until your laptop has been inspected.

The Company's Laptop User Data Recovery Responsibilities

- If the worst should happen and your laptop is stolen, lost, damaged or simply fails then it is always possible to recover your data... but only up to your last backup. It is your responsibility to ensure that you make adequate backup provision.
- When connected to The Company network, your files are automatically backed up, provided you have saved them as directed into the correct folder on your laptop.
- You should back up at least daily when working away from the company network. Use disks or USB HDDs as necessary — always encrypt and store securely. Destroy or delete out of date backup media. Do not amass backup data.
- Store backup data separately to your laptop.
- Contact the helpdesk if you need advice or require specialist or additional backup.

Laptop Policy — Software

- Your laptop is supplied with software. These are the only applications licensed for use. Do not install additional software without the express consent of the IT department.
- Be aware of Web sites and emails guiding you to download applications. You are not authorised to do so and downloaded applications may breach company policy and expose a serious security risk.
- If you need an additional application or update contact the helpdesk to discuss.

Laptop Policy — The Law

- This policy document is in addition to any applicable laws. Laptop users should be aware of any local legislation governing their use.
- Be aware of special laws governing use in flights.
- Be aware of local laws, particularly those governing content when travelling to other countries.
- Respect local laws and culture.

** Source: IDC Laptop Theft Study 2007*