FACT SHEET – Laptop Safety and Data Security

Laptops have become a valuable part of the government computing assets. These powerful and mobile computers provide connectivity, even outside the office, and are thus extremely valuable for employees who must work out-of-office or travel frequently. Unfortunately, the mobility, technology and information that make laptops so useful to employees and organisations also make them valuable prizes for thieves.

Laptop Safety

Laptops issued by Ministry/Department should be treated just as you would treat your personal precious belongings. There are some fairly simple and straightforward measures that end-users can take to safeguard their laptops against theft. These are:

- Keep the Laptop out of sight –Never leave your laptop clearly visible to the world. At the office, when the laptop is not being used, it should be safely tucked away in a locked desk drawer or cupboard even at lunchtime.
- While you are travelling by car, always put it in the car boot.
- When leaving your laptop in an unattended vehicle, make sure all doors are locked and any applicable alarm set. Never leave it in your vehicle overnight. In your home, you should make sure that the laptop is safely stored out of public view.
- If you are travelling by air, ensure that it goes as cabin luggage.
- Choose an inconspicuous carrying case - Avoid the original laptop carrying case if possible. An appropriately padded bag will do just as good a job of physically protecting the laptop.
- While travelling, laptop users should carry basic accessories only.
- Keep the laptop close at hand - Don't leave your bag unattended even for just for a minute.
- If you are at a conference, meeting or having meal, ensure that the bag containing your laptop cannot be snatched. You could put the shoulder strap under the chair leg.
- Label and Tag the Laptop and All Accessories - Make sure that everything that can be labelled is labelled with the name of the individual or organisation that owns it, and ensure that these labels are conspicuous.

Refer to *"The removal of Documents\Laptop from the Office"* section in the Government Security Instructions.

Data Security

Laptops may contain sensitive and confidential data. The information that may be lost when a laptop is stolen or lost may be invaluable or irreplaceable. The availability of such critical data to unauthorised person can result in Ministries/Departments incurring loss.

- Set a BIOS password - Laptops offer some degree of protection by having a boot password set by IT Support/DBA.
- Login Account Management - On procurement of a laptop, all unnecessary accounts (e.g. guest) should be disabled. Administrator's password must be set by IT Support/DBA. A login account with associated password must be created for each user of the laptop to log in successfully.
- Configure session timeout with a password-protected screensaver for each login account.
- Account lockout policy should be set so that after a predetermined number of unsuccessful logon attempt, the account is locked out.
- Biometrics Login - If your laptop is equipped with biometric authentication device, you should use it for authentication.

- Wireless, Bluetooth and Infrared Connectivity – All wireless connectivities should be disabled by default. No automatic association should be configured. In case wireless connectivity is required, the interface should be enabled and the wireless connection established manually. After usage, the interface must be disabled.

Technical Measures to Prevent Unauthorised Data Retrieval from laptops

Even if an unauthorised user gains access to your laptop, there are still means of protecting the information that is stored upon it.

- Disk Encryption - Tools are available to encrypt an entire mass storage device. If the disk of your laptop is encrypted, then only those parties who have permission are able to read your sensitive information.
- File Encryption - users can also opt for encryption of individual data files or directories manually. Tools are available that allow you to use strong encryption to protect information that you have stored on your hard drive.
- A freely available tool that can be used for encryption is TrueCrypt (www.truecrypt.org).

User-Level Practices for Protecting Laptop Data

The following is a list of a few things that can be done to minimise the potential loss of information in the case of laptop loss or theft.

- Use Strong Passwords – Avoid easy to guess passwords such as family name, date of birth, addresses, etc.
- Protect Your Password - You should not give out your password to anyone. Do not to write your password somewhere on your laptop, or keep it written on something stored in the laptop case.
- Store a Minimal Amount of Data on the Laptop - Store as little valuable data as possible on laptops. For out-of-office business use, take only those files that are essential for your trip.
- Store information on a removable medium. When not using the laptop, remove the removable disk and store it separately, away from the laptop or its storage bag. (Refer to Fact Sheet – Safe Practices for Portable Storage Media)
- Back up laptop data regularly - Before going on the move, back up all your data on a removable medium. Backup media should be stored independently of the laptop.

Ministries/Depts Responsibilities regarding laptops

The organisation should exercise proper responsibilities by the widespread adoption of formal approval process, policies and guidelines regarding government-owned assets as regards responsibility and accountability for assets under the care of officers.

- Formalise Issue of Assets to Officers - Use of expensive assets like laptops should be duly authorised by management. (refer to Government Security Instructions)
- Have a laptop Protection Policy in place - This document should outline the responsibility of users and how they should treat their laptop and data. All users must be fully aware of this policy when being issued with a laptop.
- Educate users - Users should be informed about the risk of carrying too much data and do regular audits to ensure that non essential data is deleted.

What to do in case of Loss/Theft of laptop?

- Report it to the Ministerial Security Officer, as per Government Security instructions, for necessary investigation.