Mobile Computing Policy - Subcontractors

The guidance and standards outlined below are designed to ensure that the information being processed, and equipment used when working on behalf of Verner Wheelock, is afforded similar levels of protection as that equipment and information that is used exclusively within the office environment. This also extends to information processed exclusively within an associate's or subcontractor's home.

General Points

- passwords will be managed in accordance with the Password Security Policy
- valuable information will be backed up to removable media and kept in a separate, but secure, location from the laptop.

1. On the Move (User)
   - Ensure that laptops are not left unattended when travelling, being particularly vigilant on public transport and in public places such as stations, airports, pubs, restaurants and hotels. At other times make sure it is left in a secure place when not in use. If possible, carry it in an inconspicuous bag rather than a laptop case with the makers name on it, such as Dell, IBM, etc.
   - If parking up for any reason, such as at a service station, ensure that all laptops and other equipment are locked away out of site, preferably in the car boot.
   - Ensure that all removable disks are carried separately from the laptop. If using a security token to permit authenticated access to a particular application, then these devices must also be carried separately from the laptop.
   - If you must use your laptop in a public place, make sure that others cannot see your work, and never process sensitive material under these circumstances.

2. Using Your Mobile Computer Securely (User)
   - If you use your laptop to communicate by email remember that information must be transmitted in accordance with Verner Wheelock security procedures.
   - Anti-virus software (with regular updates) must be installed on all laptops.
   - Ensure the system (BIOS) password facilitates have been configured to prompt for a password when the laptop is switched on.
   - Ensure that laptops are fully powered down when not in use (not just suspended), as your material may be still in memory. Remember to lock all laptops away when you return them to the office/home environment.

3. Taking Your Mobile Computer Abroad
    - Before taking your laptop abroad you should seek advice from the Information Security Management Representative or applicable supervisor.
    - Some countries prohibit the import, use and/or re-export of certain security devices e.g. encryption. If your PC has such a device and you intend taking it abroad, please seek advice on this.
    - You should be aware that there is an increased risk of your laptop being stolen when abroad, be particularly vigilant at airports when hand luggage and laptop is being X-rayed.

4. If Equipment containing data relating to Verner Wheelock clients is Lost or Stolen
    - You must report the incident immediately to the Managing Director at Verner Wheelock

5. Removable Storage
    - When using removable storage such as USBs or removable hard drives on site, always ensure that the removable storage device does not contains information relating to other audits or training courses
    - Always check at the end of an audit or training session that you have retrieved any removable storage devices and USBs and stored them securely for transportation
    - Where possible, ensure that documents or data stored on removable storage devices are encrypted or password protected

ASSOCIATE/SUBCONTRATCOR ACKNOWLEDGEMENT

I agree to abide by the Verner Wheelock Mobile Computing Policy to ensure the confidentiality, security and integrity of information being processed on behalf of Verner Wheelock.

Name:

Signed:

Date: