

## **INFORMATION SECURITY: ASSET INVENTORY CHECKLIST**

An asset inventory is important for managing insurance, theft prevention, controlling system builds, performing regular reviews and replacing older systems. The contents of an inventory listing should be drawn up using the following guidelines:

- Record all hardware serial numbers, e.g. system units, monitors, printers, network interface devices (including firewalls) etc. Recording details of keyboards, mice etc. is optional as these devices tend to move around a lot, get lost or stolen and are very low cost items.
- Record device model numbers, discs/capacities, processor/speed, memory, type of memory (for future upgrade) etc.
- Record the operating system names and version as well as the main applications installed on each device. Also record the device's role, who built/configured it, any changes made (and when), and when it was last checked.
- For other devices (e.g. telephones) you should record the model number, PDA type, accessories (car chargers etc.) as well as serial numbers.
- Software inventories should also be maintained, listing the name, version, and product number. They should also record on which device(s) the software is installed. It is best for this information to be linked to the process for managing software licensing.
- Regularly review the inventory and use it as part of a routine check on software patches, software versions, disc space requirements and service packs.
- Ensure insurance covers all assets.
- Make staff sign for equipment taken out of the office (such as laptops and mobile telephones).
- If you plan to replace systems in chronological order, record the date of purchase so you can easily identify the oldest systems.
- It is useful to record the usual physical location of a device.

## Further help and advice

### General

BERR Information Security Health Check Tool  
<http://www.securityhealthcheck.berr.gov.uk/>

BERR Information Security Home page  
[www.berr.gov.uk/sectors/infosec](http://www.berr.gov.uk/sectors/infosec)

BERR Information Security Business Advice pages  
<http://www.berr.gov.uk/sectors/infosec/infosecadvice/page10059.html>

BERR Information Security Publications (available to order or download)  
<http://www.berr.gov.uk/sectors/infosec/infosecdownloads/page9935.html>