

INFORMATION SECURITY: GOOD HOUSEKEEPING CHECKLIST

[Backup](#)

[Physical security](#)

[Education](#)

[Access control](#)

[Clear desks](#)

[Destruction](#)

[Sundry tasks](#)

[Further help and advice](#)

The frequency with which you carry out housekeeping duties may vary according to the task some activities may need to be done weekly, some monthly, some annually, depending on your particular circumstances. For instance, if you are located in a high crime area, you may wish to carry out physical security checks more often than if you were situated elsewhere.

Backup

Take backup copies of your vital information (this is fairly straightforward for computer files). This should be done regularly (daily, weekly etc.), but think about how much information you would be prepared to lose before deciding how regularly you should perform the task.

Store the backup information away from the originals (ideally in a separate location). Make sure those who might need to recover the information know where it is.

If you can't take a backup (you may have valuable documents, such as deeds or share certificates), store them in a fireproof safe or similar.

Physical Security

Keep your premises physically secure. Always ensure you know who is in the building. Prevent visitors casually wandering into your premises. If appropriate, fit an alarm. Lock valuable assets (e.g. laptops, mobiles and file servers) in a secure room. Try to keep valuable items out of direct public view.

Education

Let everyone know what is expected of them. Make sure they know the value of the information they handle and are aware of any procedures you have developed to combat threats. Make sure people know what their responsibilities are.

Access control

If you run a multi-user computer system, use the appropriate access control software to keep unauthorised persons away from information held on your computer systems. Make sure everyone who needs access has their own ID and password and ensure they can only access what they need in order to do their job.

Clear desks

Establish a practice of clearing desks at the end of each day. This need not be a complex process – simply ensure that staff have lockable drawers or cupboards in which to place their work, and make sure these are locked and the keys removed.

Destruction

If you have sensitive information which you wouldn't want to fall into the wrong hands, destroy any copies you don't need. If you have a lot of paper copies, modern shredders provide an inexpensive and effective solution. Some organisations use specialist destruction companies; this is normally only necessary if you have a lot of highly sensitive material.

Sundry tasks

- Update all virus-checker software and make sure the software is current. Remember to do this on laptops (if used) as well as desk machines.
- Make sure the software is operating as you intend.
- Go to the relevant OS/application (Microsoft Windows, Office etc.) update sites and apply all updates. Since some of these (e.g. Windows service packs) are big you may wish to save time by downloading updates and burning them to CD rather than downloading to each machine in turn.
- Change all vendor-supplied passwords on user and administrator accounts before you use them.
- Clear out temporary files and temporary Internet cache files periodically – recent versions of Windows have a wizard to do this.
- Take a backup and test it.
- Backup the system as well as the data.
- Move backup tapes off site.
- Replace backup tapes periodically.
Monitor disc space (especially on servers) and archive older files to CD, or purchase a bigger disc should storage become a problem.
- Make sure all clocks are set to the same time. Many systems do this automatically – check with your supplier.
- Periodically review all login accounts (on the network), especially admin accounts, and remove or suspend any that are not needed.
- Keep technical documentation, key holders' names/addresses etc., up to date.
- Periodically check system-event logs to see if they contain anything suspicious.
- Create an asset inventory and review and update it regularly.
- Periodically re-circulate your security policies/acceptable usage documents.
- Verify your software configurations to ensure all software is licensed.
- Make sure all door/window keys are accounted for.
- Change the alarm codes on a regular basis.
- Verify all physical controls such as window locks, cameras, doors etc., to ensure they are working and are intact.
- Ensure that CCTV tapes are working and are of good quality.
- Vacuum dust out of fan grills on sensitive equipment.

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

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>