



Frequently Asked Questions on Information Security

Q. Isn't information security IT Department's responsibility?

A. Yes and no. IT does have responsibility for securing the IT infrastructure – the networks, systems and services shared by the whole organization – but most information assets, and particularly data, belong to other parts of the business. Their security is the responsibility of nominated "Information Asset Owners" throughout the organization. Business managers and employees outside of IT are therefore largely responsible for securing our most valuable information resources.

Q. So what am I supposed to do about information security?

A. Read and comply with the information security policies, procedures and guidelines that apply to you and your handling of information: these define the main "security rules", and expand upon your legal, contractual and ethical obligations towards security. If anything is unclear, ask for help from your manager, visit the intranet Security Zone or call the IT Help/Service Desk. It's important that you understand your personal obligations.

Q. Aren't the security policies just a load of bureaucratic red tape?

A. No! We try hard to make sure the security policies and particularly the procedures and guidelines are pragmatic and easy to read. If you think we are not succeeding in that aim, let us know why and we'll do our best to help you. We are only human too!

Q. Why isn't information security completely automated?

A. We use a lot of automation but it's simply not possible to automate *all* of the security controls. Take for example the threat of "social engineering", where someone tries to trick an employee into divulging sensitive information, such as their password. Social engineers are skilled at bypassing the technical controls, exploiting our people instead.

There's also a limit to the amount of technical control we can institute without interfering too much with your work. We could insist on even longer, more complex passwords, for instance, but many of us have trouble remembering them and so would be unable to logon without calling the help desk for more password resets.

Q. I've heard that security people monitor *everything* that we do. Is that really true?

A. No, definitely not. That would be a serious privacy violation as well as highly unethical. However, you *are* personally accountable for everything that you do (or don't do!), and for everything that happens under your userID on the computer network. Therefore *some* of your activities are monitored. You may have noticed CCTV cameras in some public areas, for example.

Whenever you logon to the network, computers record the logons and track your main activities in their log files. There is more tracking of potentially dangerous transactions such as updating the General Ledger or browsing the Internet, than of routine activities such as word processing.

The logs are automatically monitored for known security issues such as spam emails or virus-infected content from the Internet, and they may also be checked manually by security staff or departmental managers for unusual and potentially unauthorized activities.

Don't forget that the security logs may just as easily prove that you were *not* engaged in some nefarious activity as proving your involvement. They simply provide evidence of what you did or didn't do. The logs can only be accessed by authorized individuals for specific purposes, and the evidence has to be interpreted properly.

Further information

For information and advice on this topic or on other aspects of information security, please speak to your manager, visit the intranet **Security Zone**, or call the IT Help/Service Desk. We're here to help.