



Developing an Information Security Policy

Why Do You Require One?

Where To Start

What To Include

Getting Help

To find out how your business could help prevent computerised attacks and increase security, contact the National e-Crime Prevention Centre:

Tel: 01902 518586

Email: Tony.Proctor@necpc.org.uk

Or visit our website: www.necpc.org.uk

Why might you want to do this?

This is a very good first question. It is a time consuming administrative task so there has to be good reason for why it is necessary. Perhaps the best way to think about it is to ask whether in your organisation or business...

- You would be able to discipline an employee who was wasting time looking at porn sites?
- Could take action against a visitor to your premises who was logging into your systems?
- You have considered the security of your information in a holistic and structured manner?
- Everyone knows who is responsible for Information Security?
- In the event of an incident (e.g. a system being hacked into), there is a known procedure to follow?
- You could demonstrate your level of information security to a potential customer requiring this?
- You are sure that you comply with laws relating to Information (e.g. the Data Protection Act).

These are just some of the issues that a documented Information Security Policy can provide tremendous help with. Simply by developing this policy you will also realise the importance of computing in your business and how you can plan so that it continues to be an effective tool for you. The overriding aim of Information Security is to prevent breaches that might result in your computer's being unavailable, bad publicity, fraud or Industrial Espionage.

How can you start?

One of the most important issues for a business is to ensure that they are operating legally. To this end, perhaps the best way to start an Information Security Policy is by looking at what you are legally obliged to do. Another fundamental approach is to identify what ICT resources you have in your company and who is responsible for them. Whichever starting point you choose, the policy needs to be a formal document that is communicated to staff and instigated and supported at the highest level within the company.

What should it include?

The suggested format that follows is in line with the Information Security Standard BS7799 / ISO 27001.

This is important as you may in the future wish to be accredited (this could be a requirement from a customer). So following these guidelines would make this process easier for your company. Bare in mind that the intention should be to develop an “Overview Document” of 2 -3 pages.

1. A Definition of Information Security

This will relate to the main principles of Information Security which are Confidentiality, Integrity and Availability (often abbreviated CIA – easy to remember). Confidentiality means that information is only available to the people for whom it is intended. Integrity means that information can only be changed by those who are authorised to do so. Availability means that the information remains available to those who have legitimate access to it.

2. A Statement expressing Management Support for the Policy

3. An overview of the application of information security as it applies to the company

This will include the legislative requirements, how staff are educated in the policy, consequences of failure to abide by the policy, the use of prevention and detection software (e.g. Anti-Virus, Firewall) and business continuity management (how the business would continue to function in terms of IT requirements if it were to experience a major problem e.g. fire or flood). It should also address the way in which third parties have access to your systems. It should classify the information used within your company (what is confidential and what is not).

4. A definition of responsibility

Who is responsible for information security management? What is the procedure for reporting incidents?

5. References to any other related documents

Any more detailed documents relating to individual systems or their use.



Developing an Information Security Policy

Where can you get help?

There is now a lot of information available on the internet relating to Information Security and a web search for "Information Security Policy" will show links to many interesting and useful sites. However, it is not always easy to determine the genuine authorities on the subject from the less credible sources.

www.necpc.org.uk is a multi-agency initiative to assist with e-crime prevention. Remember that developing a policy is one step on the ladder of information security. It needs to be acted upon and supported by procedures and systems.

www.getsafeonline.org is at the time of writing, one of the best websites for providing general advice on Information security.

It is not compulsory for you to have an Information Security Policy.....it is not compulsory for your business to survive!

Tel: 01902 518586

Email: Tony.Proctor@necpc.org.uk

Or visit our website: www.necpc.org.uk