

Starting Information Security

Think about what things are important to your business; now focus upon the things that relate to data or information, we will be concentrating on how you protect these items and this information.

Certified Digital Security Level 1



To achieve a CDS Level 1 grade of security you will need to show you have done the following:

1. Write a Policy for Managing Information and its Security (including how your staff should use email and the Internet).
2. Give everyone their own user account (protected with a password).
3. Don't use a Microsoft Windows 'Administrator' or Super User account for routine work (eg email).
4. Install an AntiVirus product (and keep it up to date).
5. Tell your staff how they need to dispose of things that may hold important information (yours or that of your customers).
6. See if the Information Commissioner's Office believes you should be Data Protection Act registered.

Certified Digital Security Level 2



To achieve a CDS Level 2 grade of security you will need to show you have also done the following:

1. Confirm your computer administrator's references and have them background checked (eg credit check).
2. Teach your users how to use computers and the Internet in a safe and secure way.
3. Keep your software and hardware up to date.
4. Keep a list of your most valuable assets.
5. Switch on your computer's logging and record keeping (where possible).
6. Get the contact details of a computer emergency callout company printed out in case the computers crash, you lose data or get hacked (this could be your normal IT Support).
7. Switch on the encryption on the wireless networks (WPA2).
8. Check for things you didn't agree to have on your network.

Certified Digital Security Level 3



To achieve a CDS Level 3 grade of security you will then need to show you have done the following:

1. Check you need and have licences for all the software installed (remove stuff you don't).
2. Ensure your computer administrators are trained to do the stuff you need them to.
3. Use an up-to-date firewall when connecting to other networks (including the Internet).
4. Dispose of things that hold data, in a way that prevent others ever reading them.
5. Plan how you would deal with a disaster or big computer problem.
6. Make sure your servers are physically secure.
7. Don't allow personal equipment on the network.
8. Limit external access to computers from the internet.