Quern House, Mill Court, Great Shelford,
Cambridge, Cambridgeshire CB22 5LD

telephone: 01223 506533
email: info@day-accountants.com

Data Security - Access

Many businesses are now completely reliant on the data stored on their Network Servers, PCs, laptops, mobile devices and cloud service providers or internet service providers. Some of this data is likely to contain either personal information and/or confidential company information.

Here we look at some of the issues to consider when reviewing the security of your computer systems with respect to access controls, and to ensure compliance with Principle 7 of the Data Protection Act. This states that -

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Access security

Good access controls to the computers and the network minimise the risks of data theft or misuse.

Access controls can be divided into two main areas:

- Physical access - controls over who can enter the premises and who can access personal data
- Logical access - controls to ensure employees only have access to the appropriate software, data and devices necessary to perform their particular role.

Physical access

As well as having physical access controls such as locks, alarms, security lighting and CCTV there are other considerations, such as how access to the premises is controlled.

Visitors should not be allowed to roam unless under strict supervision.

Ensure that computer screens are not visible from the outside.

Use network policies to ensure that workstations and/or mobile devices are locked when they are unattended or not being used.

Ensure that if a mobile device is lost it can be immobilised remotely.

Mobile devices being small are high risk items so sensitive data should always be encrypted and access to the service should be controlled via a pin number or password.

It may be necessary to disable or restrict access to USB devices and Optical readers and writers.

Finally, information on hard-copy should be disposed of securely.

Logical access

Logical access techniques should be employed to ensure that personnel do not have more access than is necessary for them to perform their role.

Sensitive data should be encrypted and access to this data controlled via network security and user profiles.

Access to certain applications and certain folders may also need to be restricted on a user by user basis.

Finally, it may be necessary to lock down certain devices on certain machines.

Passwords

A password policy consisting of a username and password is good practice.

These help identify a user on the network and enable the appropriate permissions to be assigned.

For passwords to be effective, however, they should:

- be relatively long (i.e. 8 characters or more)
- contain a mixture of alpha, numeric and other characters (such as &^")
- be changed regularly through automatic password renewal options
- be removed or changed when an employee leaves
- be used on individual files such as spreadsheets or word processed documents which contain personal information

and should NOT

- be a blanket password (i.e. the same for all applications or for all users)
- be written on 'post it' notes that are stuck on the keyboard or screen
- consist of common words or phrases, or the company name.

How we can help

We can provide help in the following areas:

- defining and documenting security and logical access procedures
- performing a security/information audit
- training staff in security principles and procedures.

Please contact us if you would like any help in any of these areas.