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. 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. The General Data Protection Regulation (GDPR) sets out the security principle, which states you must take 'appropriate technical and organisational measures' when securely processing personal data. This is also repeated as the 6th Principle of the Data Protection Act (DPA) 2018, which enhances the GDPR and also states a 'requirement that personal data be processed in a secure manner'.

For this reason preventing unauthorised or accidental access to the personal data you process is an important step towards compliance.

Access security

Good access controls to the computers and the network minimises the risk 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.

It may be necessary to block network ports via Radius servers, or other network hardware, to prevent unauthorised equipment being plugged into the network via a cable.

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, access control lists 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, either via group policy in Windows, or a third-party management application.

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. eight characters or more)
- contain a mixture of alpha, numeric and special 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

- be encrypted within your systems using a strong encryption algorithm

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
- be sent via email, unless it is just a temporary password (with no supporting information such as, what it is for and what the username is)
- not be stored as plain text within your systems.

Auditing access

Whilst not a legal requirement of the GDPR, the logging and monitoring of data (and the changes made upon it) will go a long way to supporting compliance with Article 32 of the GDPR.

Auditing your data processing will allow you to review, report and prove:

- who has accessed the data and when
- how often the data is accessed and whether this amount of access is appropriate
- in the event of accidental data loss, review what changes have been made and by whom.

Whilst both the GDPR and DPA 2018 do not state the exact measures you need to undertake, you should consider using a technical solution that is appropriate to your needs and that of the data you are processing.

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.

For information of users: This material is published for the information of clients. It provides only an overview of the regulations in force at the date of publication, and no action should be taken without consulting the detailed legislation or seeking professional advice. Therefore no responsibility for loss occasioned by any person acting or refraining from action as a result of the material can be accepted by the authors or the firm.