Think Ahead ACCA

Guide from

Wiseborne Chartered Accountants Email: info@wiseborne.co.uk
Website: www.wiseborne.co.uk
[Chartered Certified Accountants and Tax Advisers]

Keeping your data safe

Vital business information includes your customer database, marketing materials and financial records. It is key to the success of your company.

Effective data security involves understanding what data you hold and how you store and use it. You need to put in place good data security procedures, including a backup routine.

1. The data you hold

The amount of time and money you spend safeguarding your data will depend on how vital it is to your business and how likely you are to suffer a data loss. To assess the risks, you need to know what data you store and use in your company.

Establish what data you store in your business

- Many businesses store information across multiple systems and in different locations.
- Think about data held on central servers as well as information stored on laptops, staff computers, tablets and smartphones, and memory sticks. You may also have created or hold data on social networks such as Facebook.
- Consider data stored in the cloud (for example, on a service like Dropbox) and whether or not it is synchronised with one or more computers within the business.
- You may store data within your CRM or project management systems – most commonly in the form of file attachments.
- Build the most comprehensive list of data possible. Make sure you record where data is stored.
- Remember to include information stored outside of your business. For instance, your website is probably held on a server owned by a third-party hosting company, and you may use an external server for email or file storage purposes.

Examine how valuable this data is

- Mission-critical data is vital. If lost, it can seriously damage your business. You will want to give most protection to this data. This could include, for instance, your accounts data.
- Customer records and their accounting and financial data is vital and you must protect it by law.
- Mission-critical data may also include employee records and valuable market intelligence.

Look at how you use this data

- Consider who has access to the data and how often it is used or changed.
- Some data may be in constant use by many employees. For instance, your customer database.

- Other data, like staff records, may be accessed infrequently by only one or two employees.
- Think about how data is transferred. Is it sent by email, streamed online or simply moved on flash drives?
- When using online storage services like Dropbox, consider how many computers, tablets or smartphones have access to the account, as it is likely some of them will keep up-to-date local copies of the files, too.

Build up a comprehensive list of data stored in your business

- For each type of data, you should know where it is stored, how often it is accessed, and who uses it.
- You can use this list to pinpoint risks in the way your business handles data.

Your legal obligations

You must comply with the Data Protection Act

- The Act aims to ensure personal privacy, by giving individuals rights with regards to the information organisations store about them.
- Most personal information your business holds is subject to the Data Protection Act.
- If you hold personal information, you will probably have to register with the Information Commissioner's Office.
- There are some exceptions to this, but registration is straightforward.
- Even if you are exempt from registration, you must comply with eight key principles of data protection.
- Take note of the General Data Protection Regulation (arriving in May 2018), which has been drafted by the EU in an attempt to give people more control over how their personal data is used.

You can get more information about the Data Protection Act

- Find out about your data protection obligations from the Information Commissioner's Office.

2. The dangers

You could lose or damage your data through human error

- It is easy to change or erase data accidentally.
- For instance, a staff member could delete a crucial list of customers by mistake.
- Look for software with undo and rollback functions to minimise the risks posed by human error.

There are physical threats

- Failed hardware, like a broken hard disk, can result in the loss of crucial files.
- A natural disaster could destroy the server holding key business information. For example, a fire or flood in your business premises.
- Theft of company computers or mobile devices can result in data falling into the wrong hands, or being lost forever.

You could suffer a data breach online

- Hackers try to break into computers over the internet. This is a serious risk, particularly for companies that hold sensitive data.

- Some computer viruses erase files. These usually infect company systems through the internet, via a downloaded file or email.
- Other malware (malicious software) like trojans and spyware may read your data and transmit it across the internet, or wipe it completely.
- Ransomware is now a common threat, where hackers steal vital data and issue a ransom for its safe return.
- Make sure you follow good online security practice and use security software.

You could be a victim of malicious action by an individual

- Anyone with access to your data could copy or delete it.
- For instance, a disgruntled employee could sell your customer database to a competitor.
- Access control is a key way of reducing this risk. See ‘Data use’.

3. Data storage

The way you store your data is key to keeping it safe. Some storage methods are more secure than others, so you should think about where you keep your most important business data.

Storing data centrally is generally most secure

- You should consider storing your mission-critical data on a central server.
- Having data in a single place reduces the risk of theft. For instance, the risk of data being stolen is reduced because it is not stored on employee laptops.
- However, having data in one place means there is a single point of failure. If your server breaks, or cloud storage service ceases trading, your data could be inaccessible.
- To guard against this, consider mirroring the information elsewhere. Your IT supplier can help with this.
- You will need to provide a secure way for employees to use data.

In general, the risk of data loss increases the more places the data is kept

- Discourage employees from saving important data on their own computers. A single laptop theft or virus infection could be disastrous.
- Instead, provide a central filing system - either on-site or cloud-based - and give each employee named folders on your server.

Be particularly aware of the risks posed by removable media

- It is easy to lose a flash drive.
- A disgruntled employee could transfer your entire customer database to a flash drive in seconds. You can disable the USB ports on your computers to make this impossible.

Invest in multi-user cloud storage

- Sharing a single login for cloud storage services presents numerous security risks.
- Invest in multi-user cloud storage platforms by signing up to their business plans. These will provide users with their own usernames and passwords, much like you’d have on a local network, thus offering full accountability and greater security of data.

Wherever your data is stored, always take some key precautions to protect it

- Always back up your data regularly.
- Install up-to-date security software on all your computers and servers and scan regularly for viruses.
- If data is kept on a system connected to the internet, use both software and hardware firewalls to keep out hackers.
- Consider using encryption to protect your most important information. This scrambles the stored data, and is much more secure than simple password protection. Microsoft Windows has encryption built in.
- When using cloud storage, use two-factor authentication, wherever available.
- Remember physical security for in-house servers. Keep your servers in a secure room and use locks to keep laptops secure.
- Consider disposal carefully. Data stored on the hard drive of a computer, tablet or smartphone has to be erased before the device leaves the office for disposal and recycling.

4. Data use

Only give each of your employees access to the data they need

- If your staff cannot access data, they cannot change or delete it - either deliberately or by mistake.
- Make sure every employee has access to the data they need to do their job.

Use secure logins to provide different access levels

- Give each member of staff their own username and password.
- Microsoft Windows allows you to grant different access levels to particular groups or individual users.
- Make sure other business software allows you to set up staff logins too.
- Can your customer relationship management (CRM) software allow different users different levels of access?

Mobile access can be a headache

- Consider providing a virtual private network (VPN) so employees can securely connect to your company systems from outside the business.

Have clearly-defined methods for transferring data

- Data is vulnerable when in transit, whether being sent across the internet or by post. Always encrypt important data before transferring it.
- Ask your IT supplier or web host to enable security protocols such as SSL and IPSec for transferring data on the internet.
- If you are transferring data outside your business, make sure you are in compliance with data protection legislation, and that the recipient understands how they can use it.
- Make sure additional copies of data are only held for as long as necessary - whether inside or outside your company.

You may need to strike a balance between security and convenience

- Adding too many security measures can make it harder for employees to do their jobs, and encourage them to find shortcuts.
- For instance, employees with multiple passwords for multiple systems may write them down, ultimately reducing the security of those systems.
- To achieve a good balance, test out different security options and ask employees what they think.

5. Backing up data

Set up an effective backup procedure

- Backups are extra copies of data. You can use them to restore data if your working copy is lost.
- Store your backups off-site, away from the main copy of your data.
- Remember to keep backups secure too. Encrypt data, and store disks somewhere safe.
- Make sure you test your backup procedures regularly, to check that they work and you know how to recover data.

Take backups regularly

- Back up your data every day. Modern backup services (both on- and offline) offer real-time backups of files as they are accessed and modified.
- Modern backup services will schedule and manage backups automatically by offering incremental backup routines that provide multiple restore points for each file.
- If running backups manually, do so in rotation. For instance, when running daily backups, you might keep separate backups for each of the previous seven days. This allows you to roll back to a particular point in time.

Choose a backup method that suits you

- Online backup services are now the most common and enable you to store your data safely in the cloud. The responsibility of maintaining regular, incremental backups is handed to the service provider who should also offer multiple restore methods should you need to retrieve your data at any time.
- Although less common, you can also backup your data to removable disks such as portable USB hard drives or USB sticks.
- You can use a RAID system to mirror your data onto several disks. This allows you to continue working in the event of disk failure, but you need to store offsite backups, too.
- You can carry out a basic backup manually. Just copy your files onto a cloud storage service (such as Dropbox), a portable hard drive or USB stick.
- Microsoft Windows and Apple’s macOS have backup functions built in. This is adequate for basic backups and provides quick restore methods.

Ensure someone in your business has responsibility for backups

- Give one person the task of ensuring your backup procedures are functioning properly.
- Make sure they report to you regularly, and test restoring from the backups at least once a quarter.
- Ensure they also have a deputy, who can cover for absences.

6. Effective communication

Ensure everyone in your business understands the importance of data security

- Systems and processes alone are not enough to keep data secure.
- Your staff have access to the data, so they must take responsibility for its security too.

Communicate the policies and procedures which cover storing and using data

- Your employees will have to work within the guidelines you set them, so involve them in the creation of these procedures.

- Run practical workshops explaining why data security is important.
- Demonstrate how procedures should be implemented.
- Train employees in the basics of data protection law.
- If possible, make data security policies and guidelines available to all staff via the company intranet.

Seek feedback on how well the guidelines work in practice

- Review them regularly.

Signpost

- Find out about your data protection obligations from the Information Commissioner's Office (0303 123 1113).
- Register under the Data Protection Act with the Information Commissioner's Office.