HOW TO PROTECT THE IDENTITIES OF YOUR CUSTOMERS

The power of memory

www.crownrms.com

CROWN RECORDS MANAGEMENT

LIKE A LITTLE HELP TO ENSURE YOUR DATA IS MANAGED AND DISPOSED OF IN A COMPLIANT WAY? JUST FOLLOW THESE SIMPLE STEPS

There's more to data breaches than lost or stolen paperwork; information can be taken from computers, laptops and USB sticks. However, it's estimated 80% of data breaches stem from human error.

Data breaches are usually unintentionally made by individuals, so it is about taking the appropriate steps to avoid them; how businesses dispose of these devices should be a top priority. Stricter guidelines advise businesses in best practices, yet there are still many cases where companies haven't managed their records effectively and securely.

STEP 1: HUMAN ERROR

Make sure all staff know about data breaches and are aware of what is expected of them to reduce the risk of breaches, ensuring the consequences of not protecting sensitive data are understood. This responsibility also applies to temporary, as well as permanent staff.

Encourage engagement and make training fun. Incorporate team games and a short quiz to cement the message, asking staff to sign a document to confirm they have understood.

Choose data breach information champions who can act as the 'go to' person for individuals who have any queries or concerns within the organisation.

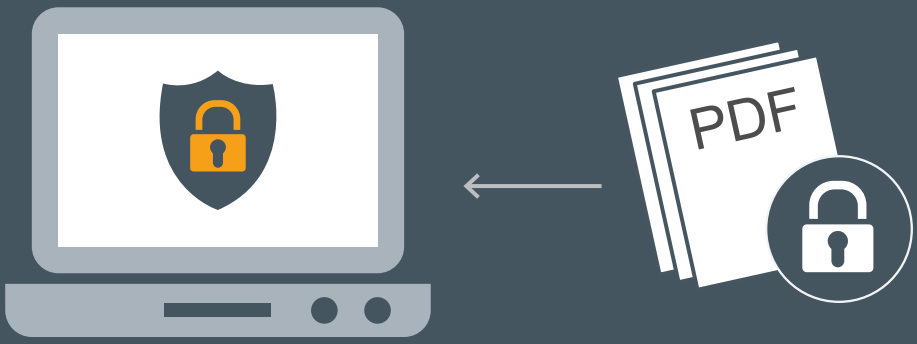
STEP 2: DATA PROTECTION

Data protection policies should be reviewed regularly, making sure they are up to date and compliant with current legislation, also bearing in mind business changes.

STEP 3: SENSITIVE DATA

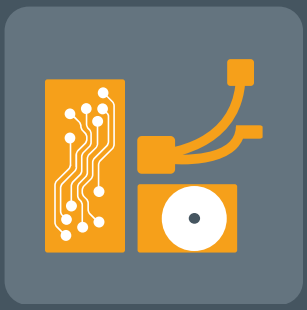
Make sure all paper files and media devices containing sensitive information are stored securely with restricted access, whether on site or with a third party.

Carry out regular back-ups of data stored on your computers and keep in a secure separate location. Access should only be given to the information employees need to do their jobs, whether online or in paper form.



STEP 4: DATA DISPOSAL

Implement a ‘shred all’ policy so staff aren’t confused as to what is confidential material, eliminating the risk of human error. Information should be wiped from all electronic devices before destruction, which should then be stored and locked away while awaiting secure disposal.



STEP 5: ENCRYPTION AND PASSWORD PROTECTION

Passwords should be changed on a regular basis, with staff aware of when to do so. Passwords should contain a minimum combination of six to eight letters and numbers, using upper and lower case, in order to reduce the risk of passwords being compromised.

Encryption strengthens data privacy and should be placed on all devices, including back-up tapes and laptops.

Information management has worked its way up the agendas of corporations, governments and institutions. Strict procedures detailing the handling and secure destruction of information should be in place. Ensure all employees are aware of their responsibility and the potential consequences of data breaches.

With these steps in place, corporate data will no longer be viewed with fear, but instead seen as a carefully protected corporate asset. It's all about being aware of the power of memory.

The power of memory

www.crownrms.com

GMO/SEP-2015/EN/V1.0