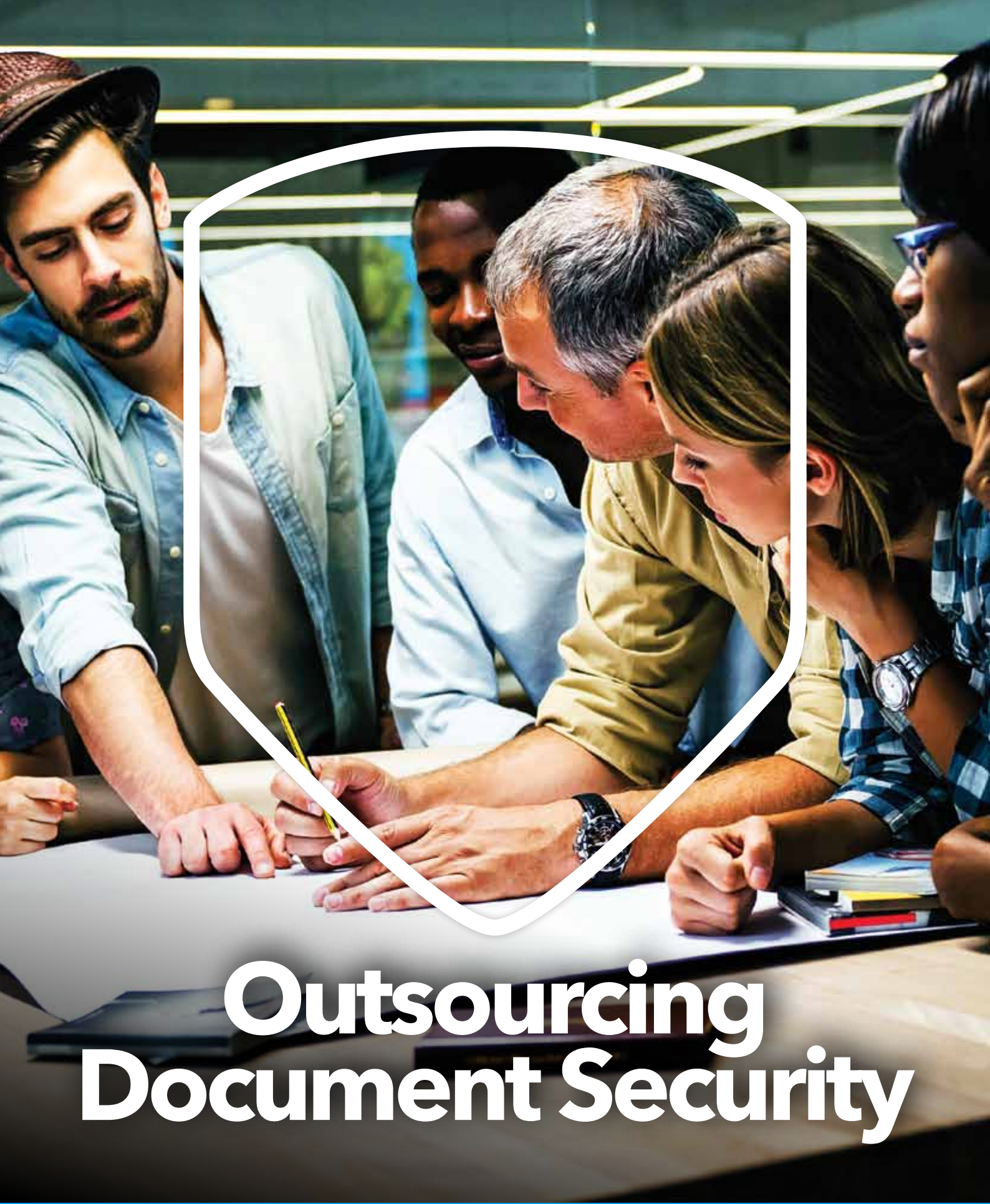
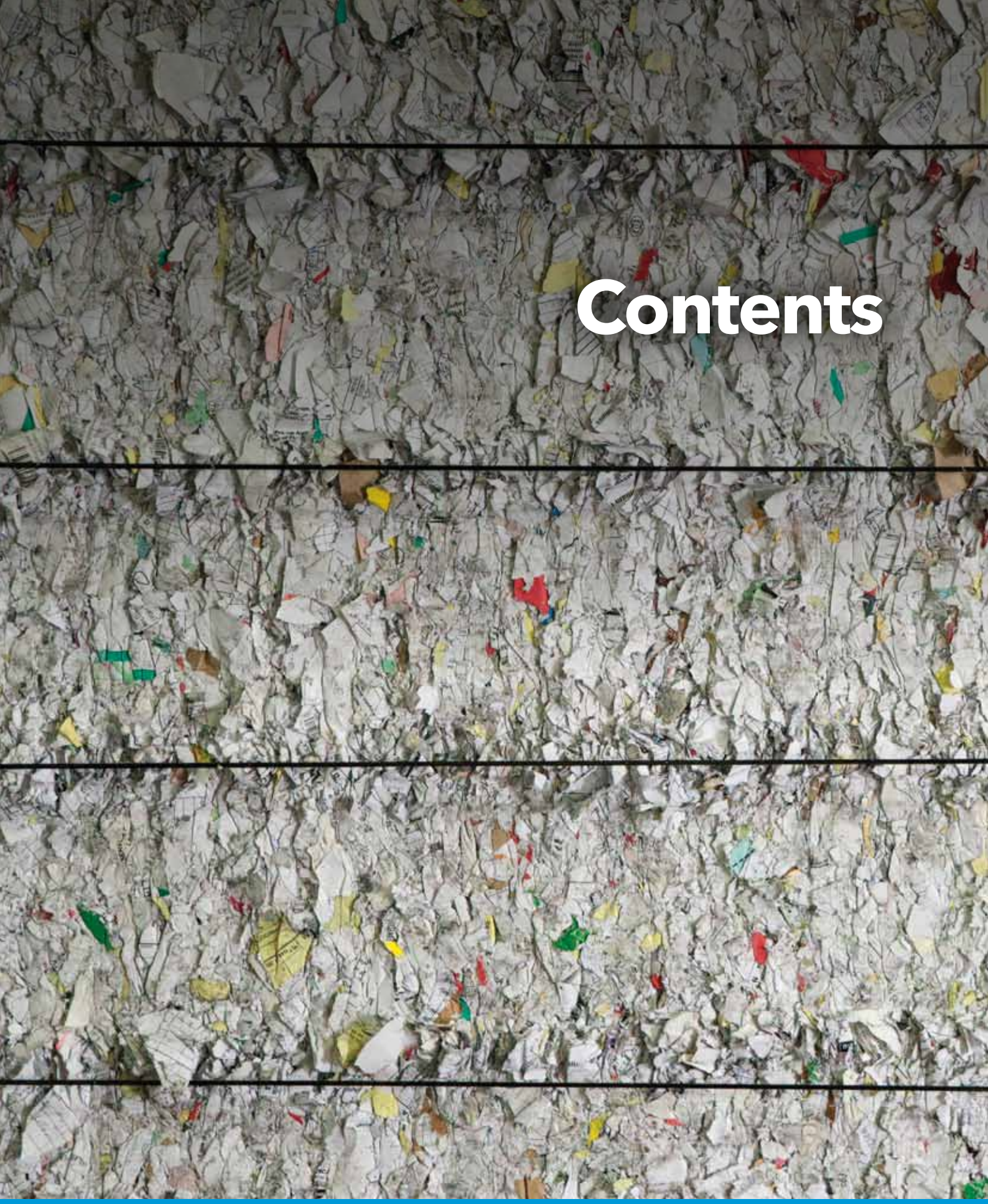


Outsourcing Document Security

United Kingdom

Shred-it®



Contents

Shred-it®

How Document Security Can "Insure" Your Company's Future

Business owners might think that a DIY approach improves security, reduces costs, saves time (and money) while better protecting privacy. They might also think that keeping document management and destruction in the hands of internal resources will provide greater confidentiality insurance.

But when it comes to boosting security, your greatest threats could lie inside your organisation. By entrusting document destruction to your employees, you could actually be increasing your risks.

In today's high-risk environment, companies are feeling more vulnerable to insider attacks than ever before and according to a survey, companies see the greatest threats coming from: privileged users (55%), contractors or service providers (46%), business partners (43%).[1]

So, the people companies trust the most (privileged insiders), pose the greatest threats to corporate security.

Here are some additional facts about threats to your corporate security you can't afford to ignore:

36% of organisations experienced economic crime in the last year[2]

5% of revenue is lost each year to fraud[3]

65% of companies don't lock up confidential information while waiting to destroy it[4]

32% of organisations never dispose of outdated USBs, hard drives and other electronic equipment[4]

5% of companies throw sensitive documents in the waste bin[4]

The threats are real and can hit your bottom line. It is estimated that the average data breach will cost a company **£2.53 million, including £1.18 million in lost sales**[5] (and the impact on the company's tarnished reputation is hard to quantify).


91% of
companies believe
they are vulnerable
to insider attacks.[6]

Office Vulnerabilities = Fraud Opportunities

There are significant threats to privacy protection in commonly overlooked areas of your office. Look around and see how many risk areas are present in your workplace.

Office Area	Why It's Vulnerable
1. Printers	Paper left on the printer can be picked up by anyone. Some printers have internal memory cards and can have documents recreated.
2. Messy Desks	Documents left on a desk can easily be seen and/or removed by anyone walking by.
3. Mobile/Storage Devices	Given their size, mobile/storage devices can be easily stolen or lost and are often without security to prevent unauthorised access.
4. Remote/Offsite Locations	When working at home or from hotel rooms (or even coffee shops), it is easy to forget security and throw out unwanted files. Home offices and other external locations don't often have locked consoles or secure storage to protect private information.
5. Recycle Bins	Documents thrown in open bins for recycling present a golden opportunity for criminals to walk by and pick out confidential information.

With real and increasing risks to businesses, how can you "insure" your future business strength?

Quite simply, it comes down to how you handle and protect the information in your possession.

34% of

UK companies have no protocol in place for storing and disposing of confidential data.[7]

Document Handling Options

Despite promises of a paperless workplace, companies are accessing and creating more confidential information than ever before (both in paper and electronic formats), which presents challenges for the secure handling of that information from the minute it is created or accessed to the time it's no longer needed.

Businesses have many options for handling documents (some of which are more secure than others). Here's a summary of some of your options, and the risks or opportunities each one presents.

Do nothing

- In today's security breach-prone environment, doing nothing to secure confidential documents puts your company at significant risk (and can irreparably damage your business).
- Doing nothing is no longer a responsible business option.

Using an office shredder

- Employees may not have training in secure document handling procedures.
- Making the decision of what is and isn't confidential is left to employee judgment.
- Manual shredding takes time and while employees are busy shredding documents, they aren't working on their priorities, which dramatically reduces productivity.
- Office shredders often produce strip-shredded material which can be recreated and is less secure.
- Documents awaiting shredding are often stockpiled until employees have time, further reducing security and presenting opportunities for theft.
- Juggling responsibilities could mean staff members have to leave shredding tasks incomplete and documents awaiting destruction unsecured.

Recycling

- Bins are open and the documents inside are accessible to anyone.
- Confidential information can be thoughtlessly thrown in the bin for recycling instead of being secured for destruction.
- Employees are left to decide what can be recycled and what needs to be destroyed.
- Confidential information leaving your office for recycling is no longer secure.

Outsourced document destruction

- Service providers are specialists in secure document handling.
- On-site Data Security Surveys are offered to identify risks to privacy.
- Providers offer a range of services tailored to specific business needs.
- Documents are handled by security-trained experts.
- Shredding technology completely destroys documents.
- All paper is recycled after securely being destroyed.
- Service providers often offer services to securely destroy electronics and e-media.
- Improved productivity by leaving document destruction to security-trained specialists.

The average worker handles 10,000 sheets of paper each year.[8]

Shred-it Information Security Professionals undergo extensive background checks and training

"Insure" Your Future

When you trust your document destruction to an outside vendor, you need to be sure you are reducing your risks, not increasing them.

Here are some tips for choosing a service provider that's effective and security conscious:

- Expertise – can help assess your security needs and service requirements to ensure legal compliance.
- Provides locked consoles for your documents.
- Employs security-screened professionals.
- Doesn't outsource collection or destruction.
- Uses handheld technology to document all material removed from your facility for shredding.
- Leverages the latest technology including cross-cut shredding.
- Offers a range of shred sizes to ensure legal and industry compliance.
- Can handle electronics to make sure they are permanently destroyed.
- Shreds everything – material is never sorted before shredding.
- Material is shredded in a secure, locked area to limit access.
- Recycles material only after it has been shredded.
- Guarantees solid chain-of-custody procedures.
- Understands and keeps up to date with data protection laws and compliance requirements.
- Provides a Certificate of Destruction after each service.

Shred-it

Layered Approach Thwarts Attempts

By reducing opportunities, you make it more difficult for criminals to access your information and steal it. When it comes to safeguarding your company from the threats of a security breach, layering your procedures is a recommended document management best practice. Secure document destruction policies are just one element of a comprehensive document management approach.

Shred-it® All Policy

By shredding every piece of paper, you're eliminating the guesswork over what is and isn't confidential information. All paper is placed in a secure console for destruction.

Key benefits:

- Improved security
- Better internal protection measures
- Eliminate guesswork
- Legal compliance
- Increased sustainability by recycling all paper after shredding

This policy eliminates human error (which accounts for 24% of security breaches) since employees don't have to decide how to handle documents.[9]

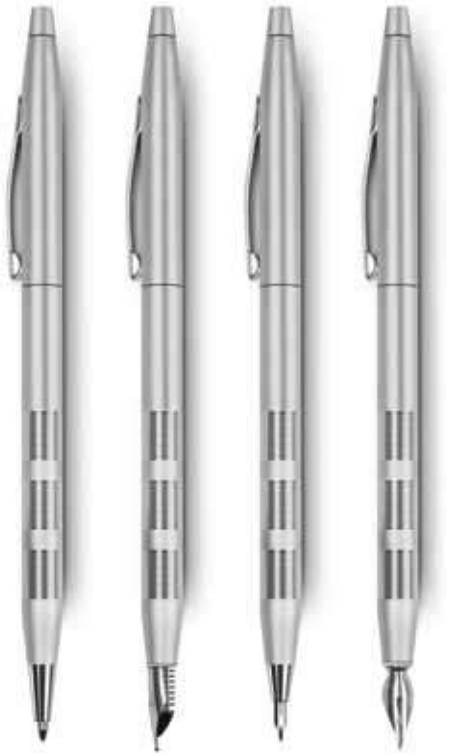
Shred-it® Clean Desk Policy

Almost every department of a company creates, accesses or uses information that could be deemed private or corporately sensitive. In many office environments, it's not unusual to walk past desks piled high with files. Those files can be easily picked up by criminals looking to profit from the information.

A Shred-it® Clean Desk Policy removes all paper from view, encourages better organisation and locks up sensitive files whenever the employee leaves, even if it is just for a short break.

Key benefits:

- Improved confidentiality and privacy protection
- All documents are secured when not in use
- Enhanced productivity
- Reduced clutter
- Paperwork is more organised and controlled
- Increased awareness around security by employees



E-Media Security

Wiping outdated hard drives doesn't eliminate the data they once contained, and locking them up isn't secure enough since someone could access the storeroom and remove the drives. An e-media destruction service ensures complete and irrecoverable hard drive destruction.

Key benefits:

- The data on hard drives is destroyed permanently
- Data can never be recreated or restored

In a test, MIT recovered

92% of

files from a sample of hard drives that had been "permanently" erased.[10]

Shred-it

How Shred-it can help

Shred-it is the global leader in information security, providing information destruction services to over 400,000 customers worldwide.

Shred-it® Solutions Secure Document and Hard Drive Destruction

- Secure end-to-end chain of custody
- Certificate of Destruction after every service
- Tailored solutions to your organisation's needs

Advice and Expertise

- Trained experts in information security
- Provide a Data Security Survey at your organisation
- Helpful resources available at shredit.co.uk/resource-centre

For peace of mind, Contact Shred-it today at 0800 028 1164 or visit us at shredit.co.uk

Sources:

1. Vormetrics. 2015 Insider Threat Report
2. PWC. Global Economic Crime Survey 2016
3. ACFE. 2016 ACFE Global Fraud Study
4. Shred-it. 2016 Security Tracker
5. Ponemon. 2016 Cost of a Data Breach Study: United Kingdom
6. Vormetrics. 2016 Data Threat Report
7. Shred-it. 2016 State of the Industry Report
8. Shred-it. Lifecycle of a Document
9. Ponemon. 2016 Cost of a Data Breach Study: Global Analysis
10. Shred-it. E-Media Disposal Process

Shred-it®