SK tes

SECURE DATA DESTRUCTION:

Onsite Shredding Checklist

When data security is of paramount importance, onsite shredding is one of the most secure data destruction methods available.

When it comes to disposing of your data storage media, such as hard drives, solid state drives, USB drives or CDs, it is important that it is done securely and responsibly.

From backing up important data and choosing a certified shredding company, to witnessing the shredding process, this checklist covers all the necessary steps to ensure the safety and security of your company's sensitive information.

1 The first step is to create an inventory of drives or other media that you want to shred, and ensure they are all accounted for.

Ensure that all data storage media is properly identified and accounted for before shredding. This is important in case any media is mistakenly left out or lost during the shredding process. Keeping an inventory of all media that needs to be shredded also helps to prevent any potential data breaches.

The most common devices that are shredded onsite include hard drives (HDDs), solid state drives (SSDs), USB drives, CDs, DVDs and floppy disks. It's important to note that not all electronic devices are suitable for onsite shredding. For example, devices that contain batteries, such as mobile phones, may require specialized handling and disposal. If you require mobile phone shredding, look for a company that offers a battery removal service prior to shredding. Some devices may be too large or complex to be shredded onsite, and may require an alternative solution.

2 Back up any important data that you wish to keep before shredding the storage media.

Make sure that all data that needs to be kept is backed up and securely transferred to a new device or storage system. Once data is shredded, it cannot be recovered, so double-check that everything still needed has been transferred.

3 Confirm that the shredding company you have chosen is certified.

If your company deals with sensitive information and you need to dispose of data bearing media, it is crucial to ensure that the company you hire has the proper certifications to ensure that your data is being handled securely.

When choosing a company for the secure onsite shredding of hard drives, it is important to look for these certifications. They provide assurance that the company has the systems in place to handle your data securely and responsibly. Here are some certifications that demonstrate high standards.

- **ISO9001** is an international standard for quality management. This certification ensures that a company has a set of processes in place to ensure consistent quality in their products and services.
- **ISO14001** is an international standard for environmental management systems. This certification ensures that a company has a robust system in place to manage its environmental impact.
- **ISO45001** is an international standard for occupational health and safety management systems. This certification ensures that a company has a system in place to manage the health and safety of its employees.
- **ISO27001** is an international standard for information security management systems. This certification ensures that a company has a system in place to manage the security of its information.

R2v3 recycling accreditation[3] is a set of standards that governs the responsible recycling of electronics. This certification is granted to companies that meet these standards, which include practices such as data security, environmental responsibility, and worker health and safety. When it comes to shredding storage media onsite, the R2v3 certification requires that companies use a secure shredding process that renders the hard drive completely unreadable and unrecoverable.

[1] Guidelines for Media Sanitization (nist.gov) [2] NAID AAA Certification - i-SIGMA (isigmaonline.org) [3] Welcome To R2v3 - SERI (sustainableelectronics.org)

4 Check that your vendor can deliver the service in accordance with industry standards and security levels.

There are several industry standards and security levels that companies may need to comply with when shredding data on electronic media. These depend on the nature of the data held on the devices, in-country jurisdiction and regulations, and specific company policies.

BS EN 15713:2023

In the UK, the standard for secure data destruction is known as the BS EN 15713:2023. This standard outlines specific requirements for the secure destruction of confidential and sensitive material, including hard disk drives. BS EN 15713:2023 provides comprehensive guidance for the management and control of material destruction including maximum particle sizes for shredding and average surface areas for the materials.

These guidelines encompass the entire process, beginning with collection and culminating in destruction, as well as including considerations for onward recycling and security measures. The standard requires that the destruction process is carried out by a reputable and licensed data destruction company, and that the company provides a certificate of destruction as proof of compliance.

NIST SP 800-88

The National Institute of Standards and Technology (NIST) in the United States also provides guidelines for data sanitization including data erasure and physical destruction of storage media with NIST SP 800-88. The NIST guide also recommends considering the National Security Agency (NSA) devices posted in the Media Destruction Guidance area of the public NSA website. NSA states:

> *"The products on these lists meet specific NSA performance requirements for sanitizing, destroying, or disposing of media containing sensitive or classified information. Inclusion on a list does not constitute an endorsement by NSA or the U.S."*

ISO/IEC 21964 - DIN 66399

ISO/IEC 21964 is the international version of DIN 66399, which sets the trend in Germany for the destruction of files and data media and has been widely adopted by international organizations. This standard provides guidelines for the destruction of data-bearing media, including the use of specialized equipment and the verification of the destruction process.

The DIN 66399 standard categorizes data into three protection classes based on the degree of protection required and determines the appropriate level of security needed to destroy the data. To ensure the secure destruction of data, the DIN 66399 specifies seven security levels, each with maximum particle sizes for various types of media, such as optical data, magnetic tapes, electronic data media and magnetic hard drives.

5 Arrange a suitable time and date for the shredding to take place.

A significant benefit of shredding onsite is that the shredding company comes to your location to shred storage devices in line with your security policies and certify them as destroyed, all without ever leaving your custody.

You will need to have sufficient parking space outside your building for shredding to take place, enough to park a lorry up to around 9m long. Ideally that will be within a reasonable distance of your entrance or docking bay. If there are any parking restrictions in your area you will need to notify the shredding company and work with them to arrange a reserved space. If you don't have suitable space your secure data destruction company should be able to suggest alternative data erasure options.

Many shredding companies require electricity to power their shredding equipment and typically bring generators or use power from your facility to operate the equipment and shred your storage media. They may ask for access to a reliable power source to complete the work.

Alternatively, some operators run their equipment from their vehicle's engine power and have no additional power requirements. This is a more convenient and much less disruptive option for most businesses and operations.

6 Decide whether you want to witness the shredding taking place.

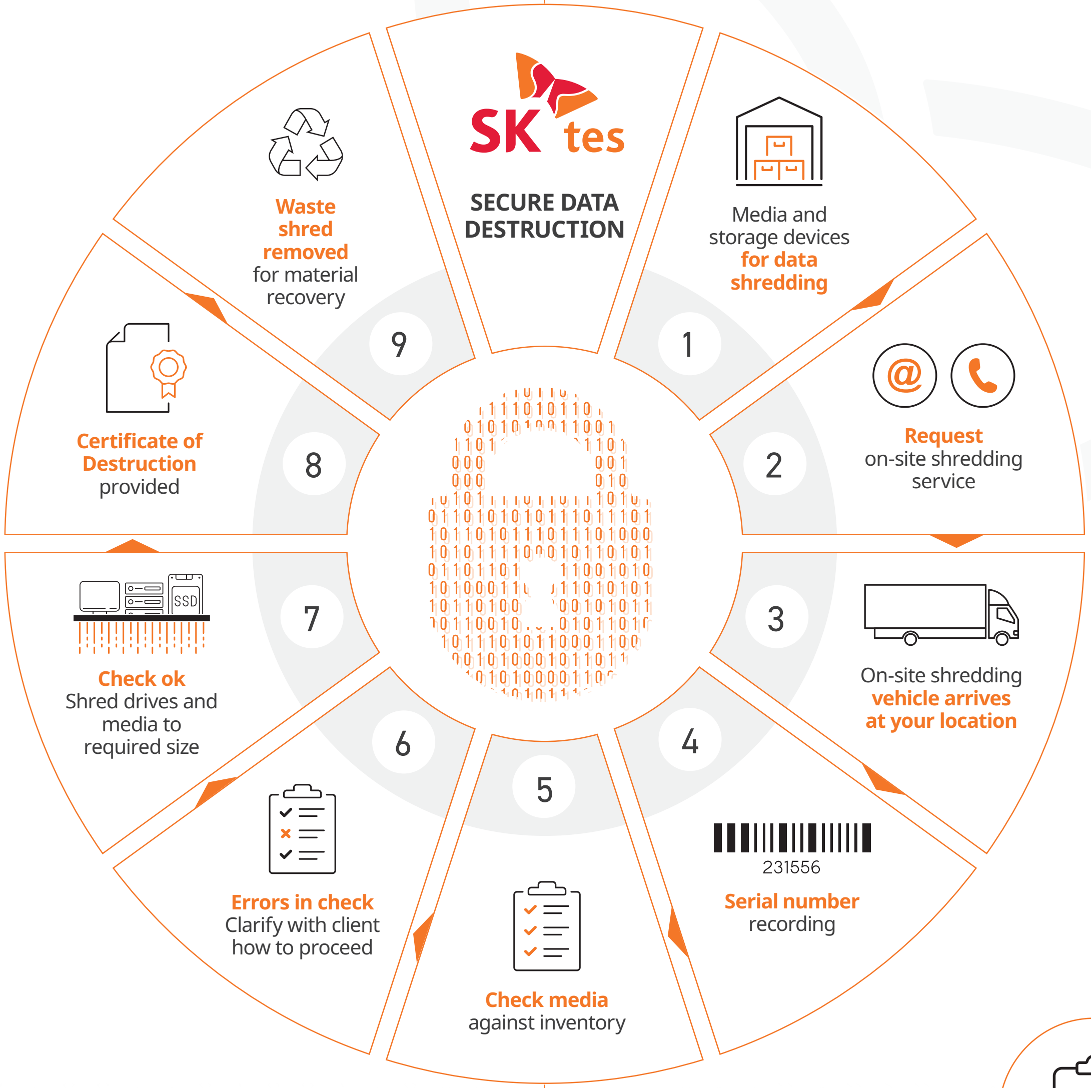
Choosing to witness onsite shredding can provide additional peace of mind and a sense of security. You can be confident that your data is being handled responsibly and that the shredding process is being conducted in a secure and professional manner.

Your organization may have strict security protocols or be subject to regulations requiring certain types of information be destroyed in a secure and verifiable manner. By witnessing the shredding yourself, you can be sure that you are meeting these requirements.

Talk to your shredding provider about viewing the shredding process. They should be able to arrange this and provide you with appropriate personal protective equipment (PPE) and a health and safety briefing before witnessing the onsite shredding. Alternatively, they may be able to video this process and provide to you when the job is complete.

7 Agree a secure process with your shredding company.

It's important to consider the security options and chain of custody to prevent any sensitive information from falling into the wrong hands. To maintain a high level of security, choose a reputable shredding service that follows strict security protocols. They should provide a secure chain of custody to ensure that drives or other storage media are tracked at all times and handled by trained professionals.



SK tes

SECURE DATA DESTRUCTION

1 Media and storage devices **for data shredding**

2 **Request** on-site shredding service

3 On-site shredding **vehicle arrives at your location**

4 231556 **Serial number** recording

5 **Check media** against inventory

6 **Errors in check** Clarify with client how to proceed

7 **Check ok** Shred drives and media to required size

8 **Certificate of Destruction** provided

9 **Waste shred removed** for material recovery

8 Plan for how long the shredding job will take.

Your chosen onsite shredding company should be able to advise you on how long the shredding job will take; this is typically dependant on the volume and type of drives being processed, and the size that they are being shredded to. Creating an accurate inventory at Step 1 will ensure that your chosen shredding service can correctly define the time your shredding will take, and provide you with up-front, clear and competitive pricing.

231556

9 Provide the shredding company with a list of serial numbers if you want your drives to be checked against that list prior to shredding.

Asset reconciliation of serial numbers can be a useful additional layer of security when shredding storage media onsite. It helps to ensure that all drives or disks are accounted for and properly disposed of, reducing the risk of data breaches. To perform asset reconciliation, you should first create a detailed inventory of all the assets being shredded, including their serial numbers. This list should then be cross-referenced against any existing IT asset management (ITAM) systems to ensure that all hard drives have been accounted for and can be removed from your asset register.

The company performing your onsite shredding should then scan and check all serial numbers of drives presented for shredding against the provided list. This final check should include a physical inspection of the shredded material to confirm that all media has been destroyed. Any media devices not present on the list should be highlighted to you by your shredding partner. Conversely, any drives scanned that are not on the set should be set aside and brought to your attention.

10 Decide what size you want your equipment to be shredded to.

When the shredding process takes place, the hard drives should be physically destroyed using specialized equipment that pulverizes the drive into tiny pieces. This ensures that all data is completely destroyed and cannot be recovered. Different media types can be shredded to different shred sizes using variable screens and reprocessing options.

When determining the size to shred hard drives to, several factors should be taken into consideration. Firstly, the nature of the data on the devices plays a crucial role. Highly sensitive or confidential information, or information that carries a government classification, may require shredding to a smaller size.

It is important to assess whether your organization is subject to any regulations regarding data disposal. Different industries and regions may have specific requirements on how data should be destroyed to maintain compliance with data protection laws.

Internal company policies on data security and disposal should also guide the decision-making process. Some organizations may have specific guidelines on the shredding sizes for various data-bearing media to minimize the risk of data breaches and protect sensitive information. By considering these aspects, you can establish an appropriate shredding size that aligns with the level of security needed for your data.

11 Confirm that the shredding company will provide a certificate of destruction once the process is complete.

Certificates of Destruction are important documents that are issued by shredding companies after they have completed the process of shredding storage media onsite. These certificates provide proof that the data has been properly destroyed and that the shredding company has fulfilled its obligation to ensure that the data is not recoverable.

These Certificates of Destruction may be required to demonstrate compliance with legal and regulatory requirements relating to data protection and the disposal of personal identifiable information (PII) and sensitive company data. Failure to comply with data protection legislation can result in hefty fines and damage to the company’s reputation.

12 Ensure that all shredded material is disposed of safely, responsibly and in compliance with waste management regulations.

While shredding is a secure practice, it can create waste that may end up in landfills. Look for a reputable and responsible shredding service that disposes of waste in an environmentally-friendly way. Some providers will leave shredded materials on-site and arrange for another company to collect later, for minimum disruption to your operational environment look for a service provider that removes this e-waste immediately for responsible disposal.

To ensure that the disposal of shredded material is done safely and in compliance with regulations, it is important to work with a reputable e-waste recycling company. They will ensure that the shredded material is properly segregated, transported, and disposed of in accordance with local regulations.

It is also important to keep records of the shredding and disposal process. This includes the data and time of shredding, the type and quantity of material shredded, and the name and contact information of the waste management company responsible for disposal. These records can demonstrate compliance with waste management regulations in case of an audit of investigation.

By following this checklist, you can ensure that the process of shredding your data bearing storage media is completed safely, securely and with minimal risk to your company data.

SK tes is an excellent choice for onsite shredding of storage media due to our commitment to environmental sustainability and expertise in electronic waste management. By choosing SK tes you can rest assured that your hard drives will be securely and thoroughly destroyed in compliance with all relevant laws and regulations.

SK tes has a track record of providing reliable and efficient onsite shredding services that are tailored to meet the specific needs of each client. Our experienced team of technicians use state-of-the-art equipment to ensure that every hard drive, CD or USB stick is shredded to a level that makes data retrieval impossible. This guarantees that your sensitive information remains confidential and safe from potential security breaches.

Alongside providing secure and reliable onsite shredding services, SK tes is committed to environmental sustainability. We take a proactive approach to electronic waste management and employ various strategies to operate with the lowest possible carbon footprint and minimize the impact of globally produced electronic waste on the environment.