CPNI
Centre for the Protection of National Infrastructure

SECURE DESTRUCTION OF SENSITIVE ITEMS

CPNI STANDARD

April 2014

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation or favour by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential, and including but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using the information contained in this document or its references. You should make your own judgment as regards use of this document and seek independent professional advice on your particular circumstances.

© Crown copyright 2014

Contents

Foreword

This document has been prepared by the Centre for the Protection of National Infrastructure (CPNI), which has the remit of providing protective security advice on behalf of the Government of the United Kingdom (UK).

The standard detailed in this document supersedes the following withdrawn standards:

- SEAP 8100 – Destruction equipment
  Security Equipment Assessment Panel, June 1998

- SEAP 8200 – Central destruction facilities
  Security Equipment Assessment Panel, June 1998

- Requirements for secure destruction – Interim standard
  CPNI, September 2012

CPNI acknowledge the design and technical support provided by Norbroch Ltd. for the production of this document.

1. Scope

This CPNI standard has been prepared to provide procedures, processes and performance monitoring that should be implemented by organisations belonging to the UK national infrastructure, including commercial enterprises, government departments (both central and local) and not-for-profit organisations (or other organisations acting on their behalf) to achieve secure destruction of sensitive items.

This standard covers the destruction process beginning with identification and categorisation of sensitive items, at the point where they are no longer required, to secure destruction. The scope of this standard does not include security of sensitive items during normal business use, safety aspects of destruction or environmental aspects of waste disposal.

The scope of the standard covers the following scenarios of destruction of sensitive items:

- Using static equipment at the location of use (item and destruction equipment co-located, such as a shredder in an office)
- Using mobile equipment at the location of use (destruction equipment is brought to the item)
- Transport followed by destruction using static equipment at an external destruction facility (the item is brought to the destruction equipment, such as use of a dedicated facility).

2. Audience

This standard is intended for all types of organisation forming part of the UK national infrastructure, including commercial enterprises, government agencies and not-for-profit organisations to assist in planning the secure destruction of sensitive items, including selection of appropriate equipment and/or a service provider.

This standard is also intended for organisations that supply secure destruction equipment and/or secure destruction services to organisations forming part of the UK national infrastructure.

This standard is intended to be applied to sensitive items assigned a government security classification (defined by the UK Cabinet Office) of SECRET or TOP SECRET; or equivalent classification as determined by the item owner.

Reader may also find that the tools and techniques described in this standard are appropriate for the secure destruction of items assigned a lower level of classification.

3. Terms and definitions

sensitive item: Any object which, if compromised, would have an adverse impact on the owner; or any individual, organisation or nation connected to the item.

owner: The organisation, individual or author to whom the sensitive item belongs.

attacker : An organisation or individual seeking to compromise sensitive items.

compromise: The result of an attacker gaining unauthorised access to sensitive items and/or the information contained therein through loss or negligence by the owner, theft, robbery or espionage.

custodian: An organisation or individual entrusted with sensitive items by the owner to act on behalf of the owner.

authorised person: A trusted individual granted unaccompanied access to sensitive items by the owner in accordance with the needs of their job.

business area: A physical space in which sensitive items are used for normal business purposes prior to destruction.

holding area: A physical space in which sensitive items that are no longer required for normal business use are stored prior to destruction.

holding container: A container in which sensitive items that are no longer required for normal business use are stored prior to destruction.

transport container: A holding container in which sensitive items are transported between the owner's site and an external storage or destruction facility.

locked: Requiring a key, token, pin, code or other access control input to open.

strong: Cannot be physically broken by an individual without tools.

waste: Output from the destruction process that is no longer sensitive. An attacker with access to waste is extremely unlikely to be able to retrieve sensitive information.

destruction: A process through which sensitive items become waste.

external destruction facility: A location away from the owner's site of normal business where static destruction equipment is housed and operated.

destruction area: A physical space in which sensitive items are processed into waste.

secure perimeter (permanent or temporary): A boundary capable of preventing an unauthorised individual without tools from gaining access.

secure destruction area: An area within an external destruction facility with a secure perimeter where sensitive items are received and destroyed.

documented procedure: A paper or electronic document available to both custodian and owner describing a process to be followed to meet an objective.

record: A paper or electronic document describing an event.

written notification: Paper or electronic communication whereby the delivery of the sensitive item(s) to the recipient is confirmed; for example a letter sent by recorded post or electronic mail where a read-receipt is received.

4. Secure destruction policy

The owner must maintain a current secure destruction policy including a documented procedure detailing at least:

- How to determine whether an item is sensitive
- If applicable, how to dismantle a sensitive item and separate non-sensitive components
- How to select appropriate methods and equipment for securely destroying sensitive items.

The owner must regularly assess that designated authorised personnel are able to correctly identify sensitive items and choose an appropriate destruction method. A record must be kept for each person containing at least:

- Assessed person's name and organisation
- Date and time of assessment
- Assessor's name and organisation
- Confirmation that the assessed person met the identification objectives.

When the designated person does not meet the identification objectives, the owner must re-assess the competence of the designated personnel and take remedial action.

5. Destruction equipment

The following requirements apply to destruction equipment and related procedures of all scales and at any location; owner's site, mobile or at an external destruction facility.

5.1 Destruction outcome

The equipment must destroy sensitive items to produce waste that is no longer sensitive. Required outcomes are detailed in Annex A (Destruction outcomes).

Where sensitive items are dismantled, any components that will NOT be destroyed must be explicitly identified by the owner and instructions given for the handling of the remaining components (see section 4).

5.2 Operation or observation by authorised personnel

Destruction equipment must be operated by authorised personnel or the operation observed by authorised personnel in line with section 6.3.

5.3 Documented training

Operators of destruction equipment must be trained and regularly assessed on the correct use of that equipment to achieve the destruction objective. A record must be kept for each operator containing at least:

- Operator's name and organisation

- Date and time of assessment
- Assessor name and organisation
- Confirmation that the operator met the destruction objective.

5.4 Operating instructions

Instructions to enable the operator to achieve the required destruction outcome must be available at the point of use of the destruction equipment.

5.5 Maintenance and performance monitoring

Destruction equipment must be serviced and maintained in accordance with the manufacturer's instructions.

Performance of equipment must be monitored to ensure that the output complies with the required destruction outcome as stated in Annex A (Destruction outcomes).

- Regular documented checks must be made, the records of which must include at least:
- Identifying serial number of equipment
- Date and time of check
- Name and organisation of the person(s) performing the check
- Description of output checked
- Confirmation of compliance or details of corrective action taken.

If performance of equipment does not comply with the required destruction outcome, corrective action must be taken and another documented check made before the equipment can be used for secure destruction.

5.6 Installation, modification and decommissioning reports

Destruction equipment must be installed within a secure destruction area, only accessible by authorised personnel.

When destruction equipment is installed, modified or decommissioned the person performing the task must produce a report detailing:

- Identifying serial number of equipment
- Date and time of action
- Name and organisation of the person(s) performing the action
- Technical description of the installation or modification sufficient to allow later integrity checks (see section 5.7).

5.7 Integrity inspections

The integrity of destruction equipment must be confirmed by an authorised person during installation, modification and thereafter at regular intervals, or in response to a security incident, to ensure that it has not been modified to facilitate an attack. Equipment must have a documented inspection schedule to include at least:

- Dates of inspections
- Procedure to be followed to verify the integrity of the equipment.

Records of integrity inspections must be kept and contain at least:

- Identifying serial number of equipment
- Date and time of inspection
- Name and organisation of the person(s) performing the inspection
- Description of the inspection, including:
    - Details of any parts of the equipment that could not be accessed
    - Observed inconsistencies
    - Any action taken as a result of the inspection.

If evidence of a possible attack is detected, compromise procedures (see section 15) must be followed.

5.8 Visibility of destruction process

It must be possible for an authorised person to visually confirm that their sensitive items have been destroyed.

6. Personnel

6.1 Non-disclosure agreement

All personnel with access to sensitive items must sign a non-disclosure agreement provided by the owner stating that they will not disclose the owner's sensitive information.

6.2 Authorisation for unaccompanied access

All personnel with unaccompanied access to sensitive items must be authorised by the owner.

The owner must have a documented procedure for authorising personnel. Records of authorised persons must be kept and contain at least:

- Person's name and organisation
- Date of authorisation
- Name and organisation of person granting authorisation
- Description of items authorised to access.

6.3 Accompanied access for personnel without appropriate authorisation

The owner may choose to grant access to sensitive items to personnel who have not been authorised in accordance with the owner's procedure (see section 6.2).

When granted access, such a person must be accompanied and observed by authorised personnel. There must be at least one authorised person for every two others.

Records of personnel granted access who have NOT been authorised in accordance with the owner's procedure must be kept and contain at least:

- Person's name and organisation
- Date of access
- Name and organisation of person granting access.

7. Storage of sensitive items selected for destruction

7.1 Storage in a holding area

Where sensitive items are stored in a holding area prior to destruction, the level of protection offered by the holding area must be at least equivalent to that provided in the business area where the items were previously stored or used.

7.2 Separation of sensitive from non-sensitive items

Sensitive items that have been selected for destruction must be stored in a separate physical space from non-sensitive items. This must be a separate room or holding container.

8. Tracking of sensitive items

Sensitive items must be tracked through the destruction process by tracking individual items or holding containers.

The owner must have documented tracking procedures that must include:

- A recorded inventory of individual items or containers of items for destruction
- Recording the date, time, location, current custodian and new custodian when each item is moved or the custodian is changed
- If transported, verifying and recording that:
    - the expected items or holding containers are loaded at the owner's site
    - tamper-evident seals are consistent and intact (see section 14) at the point of departure
    - all of the expected items or holding containers are unloaded at the external destruction facility
    - the tamper-evident seals are consistent and intact at the point of unloading and immediately before destruction
- Verifying and recording that sensitive items in holding containers or individual items are destroyed.

9. Verification of custodians and their vehicles

The owner and custodian must have a documented procedure for identifying and verifying custodians and their vehicles that must include:

- Names of expected personnel and registration numbers of expected vehicles provided in advance to the owner or current custodian with acceptable methods of communication thereof to be explicitly listed.
- Verification of personnel using photographic identification documents approved by the owner, such documents to be explicitly listed.
- Denial of access to sensitive items until all personnel and the vehicle are verified.

10. Transport of sensitive items

10.1 Separation of sensitive from non-sensitive items transported by the same vehicle

Sensitive items that have been selected for destruction must be carried in separate transport containers from non-sensitive items.

10.2 Collection from multiple sites

In a single journey, a vehicle may collect sensitive items with a common owner from multiple sites. Nothing may be unloaded from the vehicle, except at the designated destruction facility; the vehicle must NOT be used to transport items between the owner's sites.

In a single journey, a vehicle must NOT transport sensitive items belonging to different owners. There are no restrictions on vehicles transporting only non-sensitive items including waste from a mobile destruction facility.

10.3 Delivery to multiple destruction facilities

In a single journey, a vehicle may deliver sensitive items to multiple destruction facilities. Nothing may be collected from a destruction facility by the vehicle; the vehicle must NOT be used to transport items between destruction facilities.

At each external destruction facility, the inventory of unloaded items must be verified before the vehicle departs.

10.4 Security of loading and unloading areas

The sensitive items in the vehicle must be attended and observed by at least one authorised person during loading and unloading.

Loading and unloading of sensitive items must take place within a secure perimeter or, where it is not possible to establish a secure perimeter, each person loading or unloading sensitive items must be escorted by at least one unencumbered authorised person.

10.5 Transport container

Sensitive items must be transported within discreet, opaque, locked, strong containers.

Each container must be fitted with a tamper-evident seal (see section 14) and fixed or locked to the vehicle's chassis before transportation.

For closed-bodied or box vehicles, a load compartment that is not accessible from the driver's cab is considered a transport container. Open-bodied or curtain-sided vehicles cannot be considered to be transport containers but may be used to carry transport containers.

10.6 Vehicle security

The vehicle must be fitted with an audible anti-theft alarm and immobiliser, which must be armed when the vehicle is unattended. The vehicle must be fitted with a remote tracking device that makes the location of the vehicle available to the owner.

The vehicle cab must be locked at all times other than to allow the driver or passengers to enter or exit the vehicle.

10.7 Vehicle crew

Whilst transporting sensitive items, the vehicle must be attended by at least two authorised persons.

10.8 Vehicle crew communication

The crew must have a means of establishing communication with and receiving communication from the owner, the external destruction facility and the emergency services. The crew must be able to use the communication device safely and legally whilst the vehicle is in motion.

10.9 Route planning and alteration

The custodian must have a documented route plan for the vehicle, including any planned stops and business continuity procedures, which must be agreed in advance with the owner. The custodian must record any deviations from the planned route and inform the owner before or upon arrival at the destination.

10.10 Stops whilst transporting sensitive items

Whilst transporting sensitive items, the vehicle may be stopped at a location other than the owner's site or external destruction facility.

The vehicle must be stopped for less than one hour at each location. It must be attended and observed by at least one authorised person while stopped.

The crew must visually inspect the exterior of the vehicle at the end of each stop and immediately notify the owner or custodian of any indication of access or attempted access to the vehicle or transport containers. In this instance the crew must seek guidance from the owner or custodian on what action to take.

10.11 Business continuity procedures

10.11.1 Driver over-hours procedure

The custodian must have a documented procedure to minimise unplanned stops whilst transporting sensitive items due to drivers exceeding maximum legal hours.

The vehicle must not depart from the owner's site carrying sensitive items if the anticipated driving time to the destination would result in all planned drivers exceeding their legal maximum driving hours.

When unforeseen circumstances mean that all planned drivers exceed their maximum legal hours, crew replacement procedures (see section 10.11.2) must be followed.

10.11.2 Crew replacement procedure

The custodian must have a documented procedure to minimise unplanned stops whilst transporting sensitive items due to unforeseen circumstances relating to the crew.

When the planned vehicle crew is no longer able to complete the transportation of sensitive items through unforeseen circumstances such as fatigue, illness, injury or having exceeded legal maxima for driving hours, replacement crew must be available to complete the journey.

Requirements for stopping procedures (see section 10.10) must be followed. The owner must be notified of the replacement and the reason for it as soon as practicable.

10.11.3 Vehicle replacement procedure

The custodian must have a documented procedure to minimise unplanned stops whilst transporting sensitive items due to unanticipated circumstances related to the vehicle.

When a vehicle is no longer able to deliver sensitive items to the external destruction facility through unanticipated circumstances including mechanical failure or a road traffic collision, a replacement vehicle must be available.

Sensitive items must be secured by an authorised person as soon as possible. Loading into the replacement vehicle must occur within a secure perimeter. The sensitive items must be transported to a secure location agreed with the owner where an inventory must be taken.

The owner must be notified of the vehicle replacement and the reason as soon as practicable.

11. External destruction facilities

11.1 Observation

Sensitive items at the external destruction facility must be observed and attended by at least one authorised person at all times.

11.2 Secure destruction area

An external destruction facility must have a destruction area with a secure perimeter within which sensitive items are received and destroyed.

This secure destruction area may be a portion or the whole of the site of the external destruction facility.

11.3 Separation of sensitive items received from different owners

Sensitive items received from different owners must be separated within the secure destruction area. Personnel NOT authorised for access to all sensitive items in the secure destruction area must be accompanied by one or more authorised person (see section 6.3).

11.4 Timely destruction

Sensitive items must be destroyed within **24 hours** of arriving at the external destruction facility.

11.5 Business continuity procedures

The owner and destruction facility must have agreed documented procedures for when any event (including extreme weather, flooding or equipment failure) would prevent timely destruction of sensitive items.

The procedure must include:

- Details of alternative compliant facilities to which transport vehicles may travel
- Provision for the sensitive items to be transported back to the owner
- Provision for emergency storage of sensitive items at the external destruction facility if they may be neither destroyed nor transported elsewhere
- Verbal notification to the owner as soon as practicable and written notification within ten working days.

12. Mobile destruction facilities

12.1 Observation

Sensitive items processed by a mobile destruction facility must be observed and attended by at least one authorised person at all times.

12.2 Operation within secure perimeter

Mobile destruction facilities must operate within a secure perimeter. Where not possible to operate within a secure perimeter at the owner's site, a temporary secure perimeter must be established.

12.3 Vehicle security

The vehicle must be fitted with an audible anti-theft alarm and immobiliser, which must be armed when the vehicle is unattended.

13. Vehicles used for both mobile destruction and transport

A vehicle used both as a mobile destruction facility and for transporting sensitive items must comply with all requirements detailed in this document for both functions.

14. Tamper-evident seals

14.1 Suitability

Where deployed, tamper evident seals must:

- Be printed with a unique serial number
- Be sufficiently robust to remain fit for purpose in the environment in which they are deployed for the duration of use.

14.2 Procedures

The owner must have documented procedures for:

- Applying seals and recording the serial number
- Verifying the integrity of a seal
- Reporting and recording where the integrity of a seal cannot be verified (whether considered a compromise or not).

14.3 Personnel training

The owner must provide training to personnel who may apply or verify tamper evident seals during transportation of sensitive items. The training must be recorded to include at least:

- Person's name and organisation
- Date and time of assessment
- Assessor's name and organisation
- Confirmation that the trained person was correctly able to:
    - apply seals
    - verify intact seals
    - recognise seals that were not intact
    - follow reporting procedures.

15. Compromise procedures

Custodians must have documented procedures for identifying and recording suspected, potential, attempted or confirmed compromises of the sensitive items. Such procedures must include:

- Recording of all possible compromises, including where it was subsequently established that there was no compromise
- For each possible compromise, recording details of time, location, personnel, sensitive items affected and precise circumstances
- Recording of investigative and mitigating action considered and taken
- Provision of verbal notification to the owner as soon as practicable
- Provision of written notification to the owner within ten working days.

16. Use of service providers

The owner may choose to use one or more service providers to undertake destruction or transportation of sensitive items on their behalf. Each provider and any sub-contractors must comply with the requirements described in this document.

16.1 Written contract

The owner must have a written contract with a service provider. The contract must include a clause requiring the service provider to comply with this standard, and any other UK government regulations for the handling and transportation of sensitive materials.

16.2 Insurance

A service provider must hold professional indemnity insurance for the service provided and must inform the owner of the limit of indemnity.

16.3 Sub-contracting arrangements

The service provider must have the prior written approval of the owner before sub-contracting.

Where a service provider intends to sub-contract any aspect of that service, the provider must give advance written notification to the owner detailing at least:

- Name and business address of each sub-contractor (organisation or individual)
- The function to be performed by the sub-contractor.

Annex A (Destruction outcomes)

Sensitive item	Process	Required outcome
Digital memory	Cutting using a guillotine	2mm (any direction) particle
	Disintegration Hammer-milling Shredding	6mm (any direction) particle
	Incineration	Ash
	Smelting	Liquid slag or metal
Floppy disk	Bathing in chemical or acid	Remove recording surface
	Cutting using a guillotine	3mm (any direction) particle
	Disintegration Shredding	6mm (any direction) particle
	Incineration	Ash
	Smelting	Liquid slag or metal
Hard disk	Bathing in chemical or acid	Remove recording surface
	Cutting using a guillotine	3mm (any direction) particle
	Disintegration Hammer-milling Shredding	6mm (any direction) particle
	Incineration	Ash
	Smelting	Liquid slag or metal
Magnetic tape	Bathing in chemical or acid	Remove recording surface
	Disintegration Shredding	6mm (any direction) particle
	Incineration	Ash
	Smelting	Liquid slag or metal
Microform	Disintegration Shredding	2mm (any direction) particle
	Incineration	Ash
	Smelting	Liquid slag or metal
Optical disc	Cutting using a guillotine Disintegration Shredding	2mm (any direction) particle
	Grinding or scrubbing	Remove recording surface
	Incineration	Ash
	Smelting	Liquid slag or metal
Paper	Disintegration	6mm (any direction) particle
	Incineration	Ash
	Pulping	Remove all characters
	Shredding*	60mm^2
SIM or smart card	Disintegration Shredding	2mm (any direction) particle
	Incineration	Ash
	Smelting	Liquid slag or metal
Visual display unit	Disintegration Hammer-milling Shredding	6mm (any direction) particle
	Incineration	Ash
	Smelting	Liquid slag or metal

** For shredding paper printed with 12pt Times New Roman font, the width along the line of the text should be no more than 4mm, such that no more than two adjacent characters are visible on a single particle. A narrower cut width may be necessary where smaller font sizes are present.*

Annex B (Sensitive items)

Digital memory

Solid-state or programmable memory typically constructed as an array of chips mounted to a PCB component board or motherboard and used in electronic devices including:

- Computers
- Fax machines
- Graphics cards
- Hybrid Hard Drives (HHDs)
- Mobile phones
- Routers
- Secure Digital (SD) cards
- Personal Digital Assistants (PDAs)
- Printers
- Solid-State Drives (SSDs)
- Telephones
- USB sticks.

Formats include:

- Dynamic Random Access Memory (DRAM)
- Field-Programmable Gate Array (FPGA)
- Flash memory
- Read-Only Memory (ROM)
- Static Random Access Memory (SRAM).

Floppy disk

Re-writable magnetic media used with personal computers and operated by a floppy disk drive (FDD) to store a variety of electronic file types. Diskettes are available in 3.5', 5.25' or 8' formats, constructed as a thin and flexible magnetic disc sealed in a square or rectangular plastic casing lined with polyester.

Hard disk

Re-writable, non-volatile random access memory used to magnetically read and write data. Commonly found as an internal computer component, portable storage device or in servers or RAID (redundant array of independent disks) arrays. Typically constructed as one or more rigid rotating platters, a motor drive spindle and hard casing.

Formats include:

- Hard Disk Drive (HDD) with sub-formats including:
- Hybrid Hard Drive (HHD) also containing digital memory

- Integrated Drive Electronics (IDE), also known as Parallel AT Attachment (PATA)
- Serial AT Attachment (SATA)
- Small Computer System Interface (SCSI)
- ZIP disk.

Magnetic tape

Magnetic media used to record audio, video and data. Typically constructed as a long narrow plastic strip coated in a magnetisable material on a reel contained in a rigid cassette, case or cartridge.

Formats include:

- Compact Cassette (with sub-formats C60 and C90)
- Digital Audio Tape (DAT)
- Digital Video (DV) cassette
- Linear Tape-Open (LTO)
- Video Home System (VHS) cassette.

Microform

Used for micro-reproduction of documents for the purpose of storage, transmission, reading or printing. Typically rolled film on a reel, often in a cassette or mounted on a flat plastic card.

Formats include:

- Aperture cards
- Microfilm
- Microfiche.

Optical disc

Optical media used to record audio, video and data. Often re-writable. Used with personal computers to store a variety of electronic file types. Typically a flat, circular disc with a recording layer contained within a plastic substrate.

Formats include:

- Blu-Ray
- Compact Disc (CD)
- Digital Versatile Disc (DVD).

Paper

Used for writing, printing or drawing data. Available in a variety of standard sizes and weights depending on the application. Constructed from fibrous cellulose pulp, additives and coating.

SIM or smart cards

Re-writable media used for identification, authentication, data storage and application processing. Typically a plastic card containing embedded circuitry and a memory chip with metal contacts or a wire loop for data transmission. Commonly found in:

- Mobile phones
- Mobile broadband devices
- Bank cards
- Identification cards.

Visual display unit (VDU)

Used to visualise images or data generated by the connected computer, electronic or optical device. Typically a display screen with circuitry and rigid casing.

Formats include:

- Cathode Ray Tube (CRT)
- Liquid Crystal Display (LCD)
- Organic Light Emitting Diode (OLED)
- Plasma Display Panel (PDP).

Annex C (Destruction processes)

Bathing in a chemical or acid

The media (typically magnetic) is fully submerged in a bath of chemicals (typically acid) over a period of time until the recording surface has been completely removed.

Cutting using a guillotine

Media is cut by a blade which slices the material into strips of a predefined width. The sliced material is then rotated by 90° and sliced again such that a cross-cut waste material is produced.

Disintegration

Media is fed into a cutting chamber that consists of a rotating drum fitted with hardened blades rotating at high-speed against a second set of blades fixed to the inside of the chamber. Whilst in the cutting chamber, the media is subjected to cutting, abrasion and heat which gradually reduces the material particle size and destroys recording surfaces. Most disintegrators are fitted with a perforated screen that will only allow the processed material to feed through once reduced to the required particle size. Particles typically drop through the screen by gravity or may be pulled through with a vacuum pump.

Grinding or scrubbing

Typically used with optical discs, the recording surface of the disc is spun against an abrasive surface (such as an emery wheel, grinder or sanding device) until the recording layer is completely removed. Where the recording layer of the media is not exposed (such as with a DVD), the disc must be split so it may be exposed directly to the abrasive surface.

Hammer-milling

Media is fed into the mill chamber, which consists of a rotating drum fitted with hammers (typically blocks of hardened steel), which rotate at high-speed inside the chamber. Whilst in the chamber, the material is crushed or shattered under impact with the hammers, chamber wall and other media material as well as subjected to abrasion and heat. This reduces the material particle size and destroys recording surfaces. Most hammer-mills are fitted with a perforated screen that will only allow the processed material to feed through once reduced to the required size. Particles typically drop through the screen under gravity or may be pulled through using a vacuum pump.

Incineration

Media is fed into an incinerator or furnace which combusts the organic components of the media, reducing the material to ash; ‘fly ash’ and ‘bottom ash’. Fly ash takes the form of fine particles that rise with the flue gases. Bottom ash takes the forms of solid lumps of non-combustible materials, such as metals.

Pulping

Paper is fed into a pulping machine which chops and churns the material with water and chemical agents to create fibrous slurry. The slurry is then fed into a de-inking process to ensure that all characters are removed from the printed surface.

Shredding

Media is fed into a cutting chamber through a set of rotating, interlocking knives. Whilst in the cutting chamber, the media is subject to cutting, abrasion and heat which gradually reduces the material particle size and destroys recording surfaces.

Smelting

Media is typically incinerated to produce a fine ash, which is then fed into the smelting furnace at temperatures exceeding one thousand degrees Celsius. The ash melts and reacts to form liquid slag and metal that is cast, cooled and separated to allow the recovery of the metals through further recycling and refining.

Glossary

CPNI

Centre for the Protection of National Infrastructure, responsible for protecting UK national security through the provision of protective security advice. See www.cpni.gov.uk for more details.

UK

The United Kingdom of Great Britain and Northern Ireland.

National Infrastructure

Facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends.

SEAP

Security Equipment Assessment Panel; a defunct committee responsible for protective security equipment standards and assessment.

Further reading

Secure destruction of sensitive information:

www.cpni.gov.uk/advice/Physical-security/Disposal-of-sensitive-information

Contact

For further enquiries please contact CPNI at:

www.cpni.gov.uk/Contact-us

www.cpni.gov.uk

© Crown copyright 2014