



**SLOVENSKI STANDARD**  
**SIST EN 15713:2009**  
**01-oktober-2009**

---

JUfbc'i b] Yj Ub^nuLi dbY[ U[ fUX]j U!'DfUj ]UfUj bUb^U

Secure destruction of confidential material - Code of practice

Sichere Vernichtung von vertraulichen Unterlagen - Verfahrensregeln

Destruction sécurisée de documents confidentiels - Code d'usages

**Ta slovenski standard je istoveten z: EN 15713:2009**

[SIST EN 15713:2009](https://standards.iteh.ai/catalog/standards/sist/202e87b7-e3d5-43dd-8239-9c7c4d10f484/sist-en-15713-2009)

<https://standards.iteh.ai/catalog/standards/sist/202e87b7-e3d5-43dd-8239-9c7c4d10f484/sist-en-15713-2009>

**ICS:**

13.310      Varstvo pred kriminalom      Protection against crime

**SIST EN 15713:2009**

**en,fr,de**

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

SIST EN 15713:2009

<https://standards.iteh.ai/catalog/standards/sist/202e87b7-e3d5-43dd-8239-9c7c4d10f484/sist-en-15713-2009>

ICS 13.310

English Version

## Secure destruction of confidential material - Code of practice

Destruction sécurisée de documents confidentiels - Code  
d'usagesSichere Vernichtung von vertraulichen Unterlagen -  
Verfahrensregeln

This European Standard was approved by CEN on 19 March 2009.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

**STANDARD PREVIEW**  
(standards.iteh.ai)

SIST EN 15713:2009  
<https://standards.iteh.ai/catalog/standards/sist/202e87b7-e3d5-43dd-8239-9c7c4d10f484/sist-en-15713-2009>

EUROPEAN COMMITTEE FOR STANDARDIZATION  
COMITÉ EUROPÉEN DE NORMALISATION  
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: Avenue Marnix 17, B-1000 Brussels

<b>Contents</b>	<b>Page</b>
Foreword .....	3
1 Scope .....	4
2 Normative references .....	4
3 Terms and definitions .....	4
4 Company premises .....	5
4.1 Facilities .....	5
4.2 Security .....	5
5 Contracts and audit trail .....	5
6 Sub-contracting .....	5
7 Security screening of personnel .....	5
8 Collection of confidential material .....	6
9 Retention of confidential material .....	6
10 Conveyance of confidential material .....	6
10.1 Collection vehicles .....	6
10.2 On-site destruction vehicles .....	6
11 Categories of confidential material .....	7
12 End product disposal .....	7
Annex A (informative) Material specific shred and disintegration sizes .....	8

## Foreword

This document (EN 15713:2009) has been prepared by Technical Committee CEN/TC 263 "Secure storage of cash, valuables and data media", the secretariat of which is held by BSI.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by October 2009, and conflicting national standards shall be withdrawn at the latest by October 2009.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

## iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST EN 15713:2009

<https://standards.iteh.ai/catalog/standards/sist/202e87b7-e3d5-43dd-8239-9c7c4d10f484/sist-en-15713-2009>

**EN 15713:2009 (E)****1 Scope**

This European Standard gives recommendations for the management and control of confidential material destruction, to ensure that such material is disposed of securely and safely. The recommendations apply to a company's main business premises and any holding sites.

**2 Normative references**

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 50131-1, *Alarm systems – Intrusion and hold-up systems – Part 1: System requirements*

**3 Terms and definitions**

For the purposes of this European Standard, the following terms and definitions apply.

**3.1****company**

organization providing contracted services for the management and control of confidential material destruction

**3.2****client**

owner of confidential material who retains a company to provide destruction services in accordance with an agreed contract

**3.3****holding site**

non-destruction site for the secure retention of confidential material prior to the transportation to the company premises

**3.4****destruction**

reduction in size such that the material becomes, as far as is practicable, unreadable, illegible and unreconstructable

NOTE Methods of destruction include shredding and disintegration.

**3.5****shred**

reduce, by mechanical means, to a regulated size

NOTE See Annex A for material specific shred and disintegration sizes.

**3.6****disintegrate**

reduce, by mechanical means, to a regulated size less than that achievable by means of shredding

NOTE See Annex A for material specific shred and disintegration sizes.

**3.7****data processor**

any person (other than an employee of the data controller) who processes the data on behalf of the data controller

### 3.8

#### **data controller**

person who (either alone or jointly or in common with other persons) determines the purpose for which and the manner in which any personal data are, or are to be, processed

## **4 Company premises**

### **4.1 Facilities**

The company should have an administrative office and/or operational centre where records, professional and business documents, certificates, correspondence, files, etc., necessary for conducting business transactions should be kept.

The premises should be physically isolated from other business or activities on the same site.

### **4.2 Security**

An approved intruder alarm system conforming to EN 50131-1 and monitored by an alarm receiving centre should be installed in the premises. As a minimum the system should cover the processing, storage and office areas, or premises should be guarded.

A CCTV system with recording facilities should be installed to monitor the unloading, storage and processing areas with the exception of holding sites. The recorded images should be retained for a minimum of 31 days unless otherwise agreed with the client.

Authorized entry to operational areas by visitors should be subject to supervision by appropriately screened personnel. Unauthorized persons should be denied access to operational areas.

## **5 Contracts and audit trail**

<https://standards.iteh.ai/catalog/standards/sist/202e87b7-e3d5-43dd-8239-7c441918964e/sist-15713-2009>

A written contract covering all transactions should exist between the client and the company.

Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller should:

- a) choose a data processor providing sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out; and
- b) take reasonable steps to ensure compliance with those measures.

## **6 Sub-contracting**

Sub-contracted work should only be allocated to a company following the recommendations in this European Standard.

In every case the client should be informed that a sub-contractor is being used to securely destroy confidential material.

## **7 Security screening of personnel**

All staff employed in the business of secure destruction of confidential material should be security-screened in accordance with the appropriate National standard.

Prior to employment all employees should sign a Deed of Confidentiality.

**EN 15713:2009 (E)****8 Collection of confidential material**

Confidential material to be collected should be protected from unauthorized access from the point of collection to the completion of destruction.

Where possible, confidential material collected should be stored in containers secured by an individually numbered seal or security lock.

Collections should be made by uniformed and suitably trained staff carrying photographic identification.

**9 Retention of confidential material**

The destruction of confidential material should take place within one working day from arrival at the destruction centre.

**10 Conveyance of confidential material****10.1 Collection vehicles**

Vehicles should:

- a) be either box-bodied or have a secure demountable container; where a curtain-sided vehicle is used, confidential material should be transported within suitably sealed secure containers;
- b) be fitted with lockable and/or sealable doors;
- c) be able to communicate with the company by radio or telephone;
- d) be fitted with an electro-mechanical immobiliser or alarm system;
- e) be closed and locked and/or sealed during transit;
- f) be immobilised or alarmed when left unattended.

**10.2 On-site destruction vehicles**

Unprocessed confidential material should not be removed from the client's site and vehicles should:

- a) be box-bodied;
- b) be fitted with lockable and/or sealable doors;
- c) be able to communicate with the company by radio or telephone;
- d) not be left unattended when unprocessed confidential material is onboard.



## 11 Categories of confidential material

Confidential material should be categorized as shown in Table 1.

The method of destruction should be agreed with the client and suitable for the category of material in order to render it unreadable, illegible and unreconstructable.

NOTE Guidance on the destruction of confidential material, as categorized in Table 1, by specific methods is given in Annex A. The maximum cutting widths given in Table A.1 may be applied to other methods of destruction.

Table 1 — Categories of confidential material	
Category	Description
A	Paper, plans, documents and drawings
B	SIM cards and negatives
C	Video/Audio tapes, diskettes, cassettes and film
D	Computers including hard drives, embedded software, chip card readers, components and other hardware
E	ID cards, CDs and DVDs
F	Counterfeit goods, printing plates, microfiche, credit and store cards and other products
G	Corporate or branded clothing and uniforms
H	Medical X-rays and overhead projector slides
NOTE Hazardous waste is not included in this table. Users are advised of the existence of legislation applicable to the destruction and/or disposal of hazardous waste.	

## 12 End product disposal

Where practicable, end products consisting of recyclable material, e.g. paper, metal or plastics, should be recycled.

Where the end product cannot be recycled the environmental impact, cost and convenience of other methods of waste disposal, e.g. incineration, should be taken into account.

NOTE Energy can be recovered from incineration for power generation.

Landfill should be used only where no other method of disposal is practicable.