SLOVENSKI STANDARD
oSIST prEN 15713:2007

01-september-2007

Varno uniļ evanje zaupnega gradiva - Pravila ravnanja

Secure destruction of confidential material - Code of practice

Ta slovenski standard je istoveten z: **prEN 15713**

ICS:

13.310 Varstvo pred kriminalom Protection against crime

oSIST prEN 15713:2007 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 15713

August 2007

ICS

English Version

Secure destruction of confidential material - Code of practice

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/TC 263.

If this draft becomes a European Standard, 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.

This draft European Standard was established by CEN 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.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

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

Management Centre: rue de Stassart, 36 B-1050 Brussels

Ref. No. prEN 15713:2007: E

Contents

Page

Foreword

This document (prEN 15713:2007) 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 document is currently submitted to the CEN Enquiry.

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*: Intruder and hold-up alarm systems*

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

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.

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.

Annex A
(informative)
Material specific shred and disintegration sizes

Where the agreed method of destruction is shredding or disintegration, Table A.1 gives the recommended method and maximum cutting width for the categories of confidential material given in Table 1.

Table 1 – Material specific shred and disintegration sizes

Shred N°	Average surface area of material	Maximum cutting width	Method of destruction	Material categories ✓ Acceptable × Unsuitable for material							
	mm^2	mm		A	B	C	D [A]	E	F [B]	G [B]	H
1	5000	25	Shred	✓	×	✓	✓	×	—	—	✓
2	3600	60	Shred	✓	×	✓	✓	×			✓
3	2800	16	Shred	✓	×	✓	✓	×			✓
4	2000	12	Shred	✓	×	✓	✓	×			✓
5	800	6	Shred or disintegrate	✓	×	n/a	✓	✓			n/a
6	320	4	Shred or disintegrate	✓	×	n/a	✓	✓			n/a
7	30	2	Disintegrate	n/a	✓	n/a	✓	✓			n/a
8	10	0.8	Disintegrate	n/a	✓	n/a	✓	✓			n/a

[A] Materials in category D should be destroyed so that information is unreadable and subject to secure disposal.

[B] Client and material specific.