INTERNATIONAL STANDARD

ISO 11442-1

First edition
1993-09-01

Technical product documentation — Handling of computer-based technical information —

Part 1:
Security requirements

Documentation technique de produits — Gestion des informations techniques assistée par ordinateur —

Partie 1: Exigences de sécurité

Reference number
ISO 11442-1:1993(E)

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

International Standard ISO 11442-1 was prepared by Technical Committee ISO/TC 10, *Technical drawings, product definition and related documentation*.

ISO 11442 consists of the following parts, under the general title *Technical product documentation — Handling of computer-based technical information*:

— *Part 1: Security requirements*

— *Part 2: Original documentation*

— *Part 3: Phases in the product design process*

— *Part 4: Document management and retrieval systems*

International Organization for Standardization
Case Postale 56 • CH-1211 Genève 20 • Switzerland
Printed in Switzerland

Technical product documentation — Handling of computer-based technical information —

Part 1:
Security requirements

1 Scope

This part of ISO 11442 covers security aspects involved in the handling of computer-aided design (CAD) information. Such computer security is divided into four areas:

a) security with regard to installation and operation;

b) system security;

c) security with regard to document contents;

d) security with regard to communication.

Areas a) and b) apply to computerization in any form, irrespective of the subject area, and are therefore not dealt with in detail in this part of ISO 11442, with the exception of backup copying, to which special attention should be paid in computer-aided design techniques.

The use of this part of ISO 11442 is intended to facilitate:

— communication with quality assurance functions within the company and outside;

— consideration of the different security aspects in the design work;

— purchase of appropriate systems and services.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO 11442. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO 11442 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 10209-1:1992, *Technical product documentation — Vocabulary — Part 1: Terms relating to technical drawings: general and types of drawings.*

ISO/TR 10623:1991, *Technical product documentation — Requirements for computer-aided design and draughting — Vocabulary.*

3 Definitions

For the purposes of this part of ISO 11442, the definitions given in ISO 10209-1 apply. Further terminology is given in ISO/TR 10623.

4 Structural relationship of computer security

The structural relationship of the various security systems is presented schematically in figure 1.

5 Security with regard to installation and operation

NOTE 1 For access authorization, see 7.1.

5.1 Installation

Installation of computer equipment shall follow the specifications of the supplier.

5.1.1 Electricity supply

In addition to correct voltage and power, the quality of the electricity supply (protection against brief power cuts and transients) shall be considered. This applies to ordinary power as well as backup power supplies.

5.1.2 Ventilation

Adequate ventilation is required to remove heat generated by the computer.

5.1.3 Cooling

Extensive computer equipment may require separate cooling facilities.

5.1.4 Magnetism

Magnetic tapes, disks and other magnetic media shall be protected against magnetic fields.

5.1.5 Electrostatic environment

The equipment shall be protected against static electricity caused by, for example, synthetic floor coverings.

5.1.6 Trespassing

The location of computers in work areas may require reconsideration of access regulation, to reduce the risk of unauthorized access.

5.2 Operation

5.2.1 Service and maintenance

Service contracts are recommended to limit computer downtime.

5.2.2 Stand-by equipment

To eliminate, as far as possible, long computer downtimes in connection with serious equipment faults, access to suitable stand-by equipment should be guaranteed.

5.2.3 Backup copy

Original backup copying shall be carried out in accordance with established and documented routines. This ensures that entered data are not lost by, e.g., faults in the electrical system, computer malfunction or operator error. The routine shall specify personal responsibility, time schedule, storage medium and storage place, etc. Temperature and humidity control is necessary for some storage media.

Original backup copying is recommended at the end of each day for transactions carried out during the day.

Once a week as a minimum the entire database concerned should be backup-copied. The original backup copy is physically stored in a location different from that of the original document.

6 System security

6.1 Security of operation systems

6.2 Security of application systems

The computer program actually used should be regularly checked against the version that was intended to be used.

7 Security of document contents

7.1 Authorization

Rules shall be laid down concerning authorization to create/design, read/copy, check/approve, revise and phase out document contents.

These rules shall be documented with regard to, among other things, quality assurance.

The use of user identification (user ID) and passwords (or card of authorization, etc.) permits access to:

— various computer-aided activities;

— data for a product range or part of a product range;

— different document types (e.g. item list, assembly drawing).

Passwords and user IDs should not be shared. Passwords should be kept secret and changed regularly; old passwords should not be re-used.

Table 1 gives an example of a distribution of authorization levels.

Each authorized person has a unique user ID and password. The degree of authorization for the user ID shall be approved by the manager of the function area involved and shall be administered by the person in charge of the system. The user ID and password should not have any connection to name, employment number, social security number, birth date or any other related information. Passwords may include non-alphabetic as well as alphabetic characters.

For further information concerning routines for the different computer-aided activities, see ISO 11442-3.

7.2 Copyright

Because not all countries have established legislation forbidding unauthorized copying or use, each document should be provided with a clause prohibiting this.

The clause should be affixed on any document recorded on a physical support. A label containing this clause should be physically taped on the storage medium. The same clause should appear at the beginning and end of the data file when transmitted on a communication medium.

This procedure is adequate in most countries. To obtain protection in many other countries, a copyright marking is required. This marking consists of "© Company name 19XX" (where 19XX is the year in which the contents of the document were made available).

In cases where the symbol © cannot be used, it shall be replaced by the word "COPYRIGHT".

When important changes are made in the contents of the document, the original year shall be retained and shall be indicated as shown above. At the same time, the year of the revision can be given. This is not mandatory, but the copyright protection time is thereby extended.

8 Communication security

8.1 Transfer protocol checking

Check the rules according to which the data is being transferred from one application package to another. Data shall be in defined form (input/output).

8.2 Data transfer protection

The data which are being transferred shall be protected. Output data shall be in defined form.

Table 1 — Authorization in the design process

Person authorized	Create/ design	Read/copy	Check/ approve	Revise	Phase out	Document type	Product range
NNA	x	x		x	x	1	XA
NNB		x	x			1; 3	XA
NNC		x				1; 2; 3	XA
NNC		x				1; 2; 3	XB
NND	x	x		x		1	XB
NNE		x	x			1; 3	XB

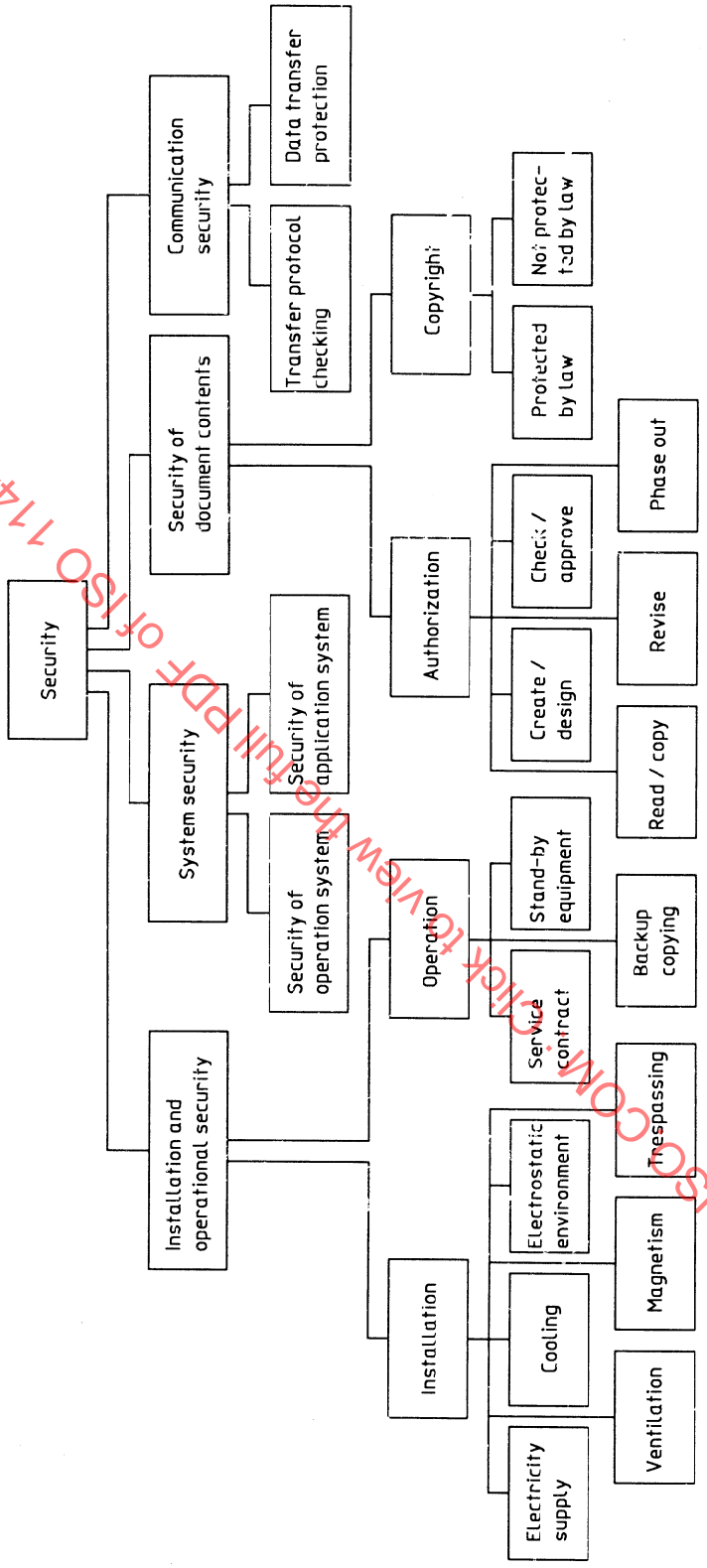

Figure 1 — Structure of computer security systems