DRAFT INTERNATIONAL STANDARD

ISO/DIS 4669-1.2

ISO/TC **171**/SC **1** Secretariat: **BSI**

Voting begins on:
2022-10-07

Voting terminates on:
2022-12-02

Document management — Information classification, marking and handling —

Part 1:
Requirements

ICS: 37.080

This document is circulated as received from the committee secretariat.

Reference number
ISO/DIS 4669-1.2:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 171, *Document management applications*, Subcommittee SC 1, *Quality, preservation and integrity of information*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Across all business sectors, there are organizations that already identify, classify and distinguish their own information and electronic communications according to their own internal rules. This classification is then used in directing the organization's staff and partners to take pre-agreed steps to use, protect and share the information, appropriate to how the organization values that information.

However, there is frequently no agreed equivalence of such classification, marking and handling amongst private sector organizations, or across the wider public sector, nor between private sector and public sector organizations. This leads to information that is shared between organizations being handled differently and sometimes inappropriately by the organizations involved.

This document encourages organizations of any size, and in any business sector, to use a managed and more consistent approach to handling information assets on the basis of their classification and marking. This approach can deliver a significant improvement in how information, and in particular sensitive information, is managed, both within the organization and within those organizations with which the information is shared. It can also contribute to the protection of the organization's investments, income, reputation and future. For example, technology companies involved in the business of information creation (e.g. typesetting or email software) that adopt and integrate the specifications in this document into their solutions will be able to create secure, automated document handling solutions, including monitoring systems, that detect and act upon the transmission of information assets that have been classified and marked.

More specifically, this document is intended to support the design of information classification, marking and handling (ICMH) systems to help organizations:

— meet their strategic objectives, governance obligations and enterprise risk management goals;

— meet legal, regulatory and standards compliance obligations;

— identify, secure, protect, share and track sensitive information appropriately; and

— improve user understanding of the value and significance of information assets and familiarity with their appropriate handling requirements.

Document management — Information classification, marking and handling —

Part 1: Requirements

1 Scope

This document specifies requirements for information classification, marking and handling (ICMH). It specifies requirements for classifying information, including defining how it can be accessed by users, both inside and outside the organization, that own the information.

This document is applicable to, but not limited to:

a) organizations of any size that create, store, share or otherwise process information;

b) individuals who create, store, share or otherwise process information;

c) individuals with responsibilities for document management, information governance and management, information security, data protection, privacy and/or compliance; and

d) organizations that create, provide or support tools that enable a) to c).

This document addresses information that can be understood by humans and is capable of being shared. Throughout this document such information is referred to as an "information asset" regardless of its media or format.

NOTE Information assets can include structured information, unstructured information, text, pictures and audio/video recordings, i.e. anything that contains information, including information that is derived from databases and turned into a tangible asset.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
classification
systematic identification and/or arrangement of *information assets* (3.7) into categories according to logically structured conventions, methods and procedural rules

Note 1 to entry: These categories consider such issues as the sensitivity of an *information asset* (3.7) to loss or damage, i.e. confidentiality, integrity and availability and other impacts on the organization(s).

[SOURCE: ISO 15489-1:2016, 3.5, modified — “information assets” has replaced “business activities and/or records” and Note 1 to entry has been added.]

3.2
document
information (3.6) and the medium on which it is contained

[SOURCE: ISO 9000:2015, 3.8.5, modified — The example and notes to entry have been deleted.]

3.3
handling
required activities relating to *information assets* (3.7) that have been marked with a specific *classification* (3.1)

3.4
information classification, marking and handling scheme
ICMH scheme
respective, specific requirements and arrangements established for the individual activities of *classification* (3.1), *marking* (3.10) or *handling* (3.3)

3.5
information classification, marking and handling system
ICMH system
set of interrelated or interacting elements to establish information *classification* (3.1), *marking* (3.10) and *handling* (3.3) policies and objectives with processes to achieve those objectives

3.6
information
meaningful data

Note 1 to entry: Data can be regarded as lacking the context necessary to interpret its meaning. Information is accurate and timely, specific and organized for a purpose, presented within a context that gives it meaning and relevance, and can lead to an increase in understanding and decrease in uncertainty. Information is valuable because it can affect behaviour, a decision or an outcome.

[SOURCE: ISO 9000:2015, 3.8.2, modified — Note 1 to entry has been added.]

3.7
information asset
set of *information* (3.6) that is capable of being shared and can be held in any form, e.g. physical or digital

3.8
information asset life cycle
sequence of events that mark the development and use of an *information asset* (3.7)

[SOURCE: ISO/TS 13972:2015, 2.33, modified — “asset” has replaced “resource” and the example has been deleted.]

3.9
information provider
individual or entity that has shared *information* (3.6) with the organization

Note 1 to entry: This includes *workers* (3.18) within an organization when, for example, referring to them as natural persons. Otherwise it relates to third parties.

3.10
marking
process by which a *classification* (3.1) is documented and indicated for an *information asset* (3.7) (usually on the *information asset* (3.7))

3.11
metadata
data about data

Note 1 to entry: Metadata (see ISO 23081-1) is contained in many *information assets* (3.7) and describes the *information asset* (3.7). *Information classification* (3.1), *marking* (3.10) and *handling* (3.3) (ICMH) technologies and tools commonly use metadata to convey classifications. Without the use of such technologies, metadata is not always immediately visible and possibly will not be automatically transferred when the *information* (3.6) changes format.

3.12
physical storage media
physical device on which *information* (3.6) can be recorded

3.13
record
information (3.6) created or received and maintained as evidence and as an asset by an organization, in pursuit of legal obligations or in the course of conducting business.

Note 1 to entry: Records are normally used in plural.

[SOURCE: ISO 30300:2020, 3.2.10]

3.14
redaction
permanent removal of *information* (3.6) within a *document* (3.2)

[SOURCE: ISO/IEC 27038:2014, 2.4]

3.15
render
action of converting data into a human-perceivable form

[SOURCE: ISO/IEC 21000-19:2010, 3.1.49, modified — “data into” has replaced “a resource to”]

3.16
replication
digital duplication where there is no change to the *information* (3.6)

[SOURCE: ISO/TS 21547:2010, 3.1.26]

3.17
storage media
device on which digital *information* (3.6) can be stored

3.18
worker
individual working under the control of an organization, including employees, temporary staff, contractors and consultants

4 Principles

The ICMH system shall include a definition of a process for the handling of information in a way appropriate to its classification and to its marking.

The organization shall ensure that its ICMH system:

a) is as simple as the circumstances allow;

NOTE 1 An overly complex process can be difficult for a small company to apply and a simplistic process does not always suit the complexity required in a large organization.

b) reflects the sensible limits of what can be expected of its workers such that they can achieve an appropriate balance of what shall, should and would be appropriate to be achieved;

c) produces consistent results upon repeated use, regardless of the user;

d) is traceable and capable of verification;

e) is usable by both human and automated systems;

f) is usable for purely manual processes (e.g. paper-based), as well as fully- or partially-automated processes;

g) addresses all relevant security attributes;

h) takes account of, and where appropriate, replaces existing ICMH systems;

i) supports compliance with internal and external requirements;

j) is resilient to changes in circumstances, technology and systems;

NOTE 2 Organizations might need to augment an original scheme, e.g. with additional descriptors, as the role or coverage of an ICMH system evolves. This does not necessarily mean that the ICMH system as a whole needs to change.

k) takes account of changes in the nature and sensitivity of information over time;

l) is applied throughout the lifetime and life cycle of the information asset.

The organization shall ensure that its ICMH system is consistent with the organizations overall information management policies and procedures.

Consideration shall be given to all opportunities open to it to facilitate effective handling, including simplifying the arrangements as much as possible and supporting them with technology as appropriate.

5 ICMH system design

5.1 Classification scheme design

5.1.1 Classification criteria

The ICMH system shall include a specification of a classification scheme, detailing how information shall be classified, and by whom, such that people with authorized access to information can mark and handle the information in a consistent manner.

Information shall be classified according to:

a) the assessed direct and indirect value of the information itself to the organization(s) involved;

b) the risk of inappropriate disclosure, corruption, loss of or loss of access to the information asset, and the organization's appetite to accept such risk(s);

c) the related costs to the organization of identified risk events occurring and resulting in negative impacts such as harm to members of the public, reputation damage, the costs of rectification and of mitigation;

d) the expectations of stakeholders who are not necessarily directly engaged in the information asset but whom nonetheless have the authority to impose requirements, e.g. legislation and regulation;

e) the need to control the extent of access to the information asset throughout its life cycle;

f) the delivering of coherence with, and mapping between, classifications and risk levels used in the organization's risk management process;

g) the amount of effort required to protect the information asset;

h) the specific expectations of other organizations with which information assets are shared;

i) the general expectations of other parties, such as members of the public and journalists, etc., even when the information is not being shared;

j) social responsibility obligations and/or aspirations of the organization.

The ICMH system shall specify what action workers shall undertake if they:

— cannot make an assessment of classification;

— cannot comply with the requirements of the classification, e.g. for legal or practical reasons;

— consider the classification assigned to and marked on an information asset to be incorrect.

Consideration shall be given to its decision regarding the impact of classification changes on the authenticity and/or integrity of the information.

The ICMH system shall define:

— the procedures to mitigate the impact of classification changes on the authenticity and/or integrity of the information;

— the range and extent of changes to classification that may be performed by workers on each class of information asset throughout its life cycle.

The justification for the classification scheme shall be documented and traceable.

NOTE Annex A provides example classification, marking and handling schemes. Annex B provides examples and detailed guidance when applying the ICMH system to information assets in different formats and/or media.

5.1.2 Hierarchy

Information shall be classified according to a hierarchy. The number of classes in this hierarchy shall be specified.

NOTE 1 Typically, a hierarchy of access restrictions ranges from “restricted access” to “unrestricted access”. For a brief example of a hierarchy, see Table 1. For a more detailed example, see Annex A.

Consideration should be given to the usability of the hierarchy. In general, fewer classes will be simpler to use and more likely to be used correctly.

The names of the classes in this hierarchy shall be specified.

NOTE 2 One example of a hierarchy can include highly sensitive, sensitive, not sensitive and intended for publication.

The hierarchical classes should have meaningful names. For example, defining a hierarchy of “not sensitive” to “highly sensitive” is likely to be more helpful than defining a hierarchy of numbers “1” to “5”.

NOTE 3 If all information is classified at the highest level, the efficiency of an organization can be reduced. If all information is classified as having unrestricted access, it is likely that this would cause harm to the organization.

Table 1 — Example of a confidentiality hierarchy

Class	Description
Highly sensitive	This information is the most sensitive held by an organization and great care should be taken to avoid it being accessed (accessed rather than shared because sharing implies a conscious act) inappropriately as this can cause great harm to the organization.

Table 1 *(continued)*

Class	Description
Sensitive	This information is not as sensitive as highly sensitive information but can nonetheless do harm if accessed inappropriately.
Internal	This information is private to an organization but unauthorized access to the information within it is unlikely to do significant harm.
Public	This information is intended for public dissemination.
Non-sensitive	All other information or information assets that are not classified as the information in them is trivial and access to it poses no danger to the organization.

NOTE 4 A more detailed example of a hierarchy is given in Table A.1.

5.1.3 Classification scheme equivalence

When working with a third party involves exchanging or sharing information, the organization shall:

a) explain their ICMH system to the third party so that the third party understands the significance of the system and associated schemes and the organization's requirements for classification, whether or not the third party has a classification scheme;

b) agree and document the equivalence between the organization's and the third party's schemes whenever possible;

c) agree and document how information that is exchanged or shared will be classified and consequently marked and handled by the third party.

When creating or updating a classification scheme, the equivalence of its ICMH schemes with the schemes of third parties with whom they exchange or share information shall be preserved.

Consideration should be given to how technology can be used to ensure reliable and consistent mapping between these schemes and enforcement of control rules, and if the rules are conducive to technology use.

5.1.4 Information asset life cycle

The classification scheme shall be continuously applied throughout the information asset's life cycle and shall be managed from creation or capture to eventual disposal, which can be many years later.

NOTE 1 It is not uncommon for there to be changes to the classification of specific information, and consequently its marking and handling, throughout the information asset life cycle organization (e.g. from a high degree of control to lower, more relaxed access control).

Where an expected classification change is pre-planned, the triggers, procedures and organizational rules for such future change shall be preserved. This shall ensure that the information is linked to the appropriate triggers, procedures and rules.

NOTE 2 Changes to classification can be pre-planned or unforeseen. For pre-planned changes to classification, there is typically a trigger that initiates the future re-classification; such a trigger is typically a date, a period or a specific event.

The ICMH system shall define the information to be created and retained for planned and unplanned changes in classification of information assets, such that evidence of such changes is available when required.