

<b>STN</b>	<b>Informačné technológie Bezpečnostné metódy Rámec pre riadenie prístupu (ISO/IEC 29146: 2024)</b>	<b>STN EN ISO/IEC 29146</b>  97 4133
------------	---	--

Information technology - Security techniques - A framework for access management (ISO/IEC 29146:2024)

Táto norma obsahuje anglickú verziu európskej normy.  
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 05/26

Obsahuje: EN ISO/IEC 29146:2026, ISO/IEC 29146:2024

Oznámením tejto normy sa ruší  
STN EN ISO/IEC 29146 (97 4133) z júla 2023

**142532**

---

Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2026  
Slovenská technická norma a technická normalizačná informácia je chránená zákonom č. 60/2018 Z. z. o technickej normalizácii  
v znení neskorších predpisov.

EUROPEAN STANDARD

EN ISO/IEC 29146

NORME EUROPÉENNE

EUROPÄISCHE NORM

March 2026

ICS 35.030

Supersedes EN ISO/IEC 29146:2023

English version

## Information technology - Security techniques - A framework for access management (ISO/IEC 29146:2024)

Technologies de l'information - Techniques de sécurité  
- Cadre pour gestion d'accès (ISO/IEC 29146:2024)

Informationstechnologie - Sicherheitstechniken - Ein  
Rahmenwerk für die Zugangsverwaltung (ISO/IEC  
29146:2024)

This European Standard was approved by CEN on 20 March 2026.

This European Standard was corrected and reissued by the CEN-CENELEC Management Centre on 29 April 2026.

CEN and CENELEC 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-CENELEC Management Centre or to any CEN and CENELEC 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 and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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



**CEN-CENELEC Management Centre:  
Rue de la Science 23, B-1040 Brussels**

**EN ISO/IEC 29146:2026**

<b>Contents</b>	<b>Page</b>
<b>European foreword.....</b>	<b>3</b>

## **European foreword**

The text of ISO/IEC 29146:2024 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 29146:2026 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

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 September 2026, and conflicting national standards shall be withdrawn at the latest by September 2026.

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

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

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

## **Endorsement notice**

The text of ISO/IEC 29146:2024 has been approved by CEN-CENELEC as EN ISO/IEC 29146:2026 without any modification.



# International Standard

**ISO/IEC 29146**

## Information technology — Security techniques — A framework for access management

*Technologies de l'information — Techniques de sécurité — Cadre  
pour gestion d'accès*

**Second edition  
2024-01**

## ISO/IEC 29146:2024(en)



### **COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

**ISO/IEC 29146:2024(en)****Contents**

Page

<b>Foreword</b> .....	<b>iv</b>
<b>Introduction</b> .....	<b>v</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Abbreviated terms</b> .....	<b>4</b>
<b>5 Concepts</b> .....	<b>5</b>
5.1 A model for controlling access to resources.....	5
5.1.1 Overview.....	5
5.1.2 Relationship between identity management system and access management system.....	6
5.1.3 Security characteristics of the access method.....	7
5.2 Relationships between logical and physical access control.....	7
5.3 Access management system functions and processes.....	8
5.3.1 Overview.....	8
5.3.2 Access control policy.....	8
5.3.3 Privilege management.....	9
5.3.4 Policy-related attribute information management.....	10
5.3.5 Authorization.....	11
5.3.6 Monitoring management.....	12
5.3.7 Alarm management.....	12
5.3.8 Federated access control.....	13
<b>6 Reference architecture</b> .....	<b>14</b>
6.1 Overview.....	14
6.2 Basic components of an access management system.....	15
6.2.1 Authentication endpoint.....	15
6.2.2 Policy decision point.....	15
6.2.3 Policy information point.....	15
6.2.4 Policy administration point.....	16
6.2.5 Policy enforcement point.....	16
6.3 Additional service components.....	16
6.3.1 General.....	16
6.3.2 Subject centric implementation.....	16
6.3.3 Enterprise centric implementation.....	18
<b>7 Additional requirements and concerns</b> .....	<b>19</b>
7.1 Access to administrative information.....	19
7.2 AMS models and policy issues.....	19
7.2.1 Access control models.....	19
7.2.2 Policies in access management.....	19
7.3 Legal and regulatory requirements.....	20
<b>8 Practice</b> .....	<b>20</b>
8.1 Processes.....	20
8.1.1 Authorization process.....	20
8.1.2 Privilege management process.....	20
8.2 Threats.....	21
8.3 Control objectives.....	22
8.3.1 General.....	22
8.3.2 Validating the access management framework.....	22
8.3.3 Validating the access management system.....	24
8.3.4 Validating the maintenance of an implemented AMS.....	28
<b>Annex A (informative) Common access control models</b> .....	<b>31</b>

**ISO/IEC 29146:2024(en)****Foreword**

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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 document 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](http://www.iso.org/directives) or [www.iec.ch/members\\_experts/refdocs](http://www.iec.ch/members_experts/refdocs)).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at [www.iso.org/patents](http://www.iso.org/patents) and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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](http://www.iso.org/iso/foreword.html). In the IEC, see [www.iec.ch/understanding-standards](http://www.iec.ch/understanding-standards).

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 29146:2016), of which it constitutes a minor revision. It also incorporates the Amendment ISO/IEC 29146:2016/Amd.1:2022. The changes are as follows:

- the text has been editorially revised and normative references updated.

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](http://www.iso.org/members.html) and [www.iec.ch/national-committees](http://www.iec.ch/national-committees).

**ISO/IEC 29146:2024(en)****Introduction**

Management of information security is a complex task that is based primarily on a risk-based approach and that is supported by several security techniques. The complexity is handled by several supporting systems that can automatically apply a set of rules or policies consistently.

Within the management of information security, access management plays a key role in the administration of the relationships between the accessing party (subjects that can be human or non-human entities) and the information technology resources. With the development of the Internet, information technology resources can also be located over distributed networks. The management of access is expected to comply to a policy and to have common terms and models defined in a framework.

Identity management is also an important part of access management. Access management is mediated through the identification and authentication of parties that seek to access information technology resources. Access management relies on the existence of an underlying identity management system.

A framework for access management is one part of an overall identity and access management framework. The other part is the framework for identity management, which is defined in the ISO/IEC 24760 series.

This document describes the concepts, actors, components, reference architecture, functional requirements and the practice of an access control framework.

The document focuses mainly on the access control for a single organization. It provides additional considerations for access control in collaborative arrangements across multiple organizations. The document includes examples of access control models.

# Information technology — Security techniques — A framework for access management

## 1 Scope

This document defines and establishes a framework for access management (AM) and the secure management of the process to access information and information and communications technologies (ICT) resources, associated with the accountability of a subject within some contexts.

This document provides concepts, terms and definitions applicable to distributed access management techniques in network environments.

This document also provides explanations about related architecture, components and management functions.

The subjects involved in access management can be uniquely recognized to access information systems, as defined in the ISO/IEC 24760 series.

The nature and qualities of physical access control involved in access management systems are outside the scope of this document.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

ISO/IEC 24760-1, *Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts*

ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*

**koniec náhľadu – text ďalej pokračuje v platenej verzii STN**