SVENSK STANDARD
SS-EN ISO/IEC 27001:2023

Informationssäkerhet- Cybersäkerhet och integritetsskydd - Ledningssystem för informationssäkerhet - Krav (ISO/IEC 27001:2022)

Information security, cybersecurity and privacy protection - Information security management systems - Requirements (ISO/IEC 27001:2022)

Svenska Institutet för Standarder

Språk: svenska/Swedish
Utgåva: 2

Denna standard är såld av
SEK Svensk Elstandard som även lämnar
allmänna upplysningar om svensk och utländsk standard.
Postadress: SEK, Box 1042, 172 21 Sundbyberg
Telefon: 08-444 14 00.
E-post: sek@elstandard.se Internet: elstandard.se

Svenska Institutet för Standarder

Den här standarden kan hjälpa dig att effektivisera och kvalitetssäkra ditt arbete. SIS har fler tjänster att erbjuda dig för att underlätta tillämpningen av standarder i din verksamhet.

SIS Abonnemang
Snabb och enkel åtkomst till gällande standard med SIS Abonnemang, en prenumerationstjänst genom vilken din organisation får tillgång till all världens standarder, senaste uppdateringarna och där hela din organisation kan ta del av innehållet i prenumerationen.

Utbildning, event och publikationer
Vi erbjuder även utbildningar, rådgivning och event kring våra mest sålda standarder och frågor kopplade till utveckling av standarder. Vi ger också ut handböcker som underlättar ditt arbete med att använda en specifik standard.

Vill du delta i ett standardiseringsprojekt?
Genom att delta som expert i någon av SIS 300 tekniska kommittéer inom CEN (europeisk standardisering) och/eller ISO (internationell standardisering) har du möjlighet att påverka standardiseringsarbetet i frågor som är viktiga för din organisation. Välkommen att kontakta SIS för att få veta mer!

Kontakt
Skriv till kundservice@sis.se, besök sis.se eller ring 08 - 555 523 10

Upplysningar om sakinnehållet i standarden lämnas av Svenska institutet för standarder, telefon 08 - 555 520 00. Standarder kan beställas hos SIS som även lämnar allmänna upplysningar om svensk och utländsk standard.

Standarden är framtagen av kommittén för LIS, SIS/TK 318/AG 11.

Har du synpunkter på innehållet i den här standarden, vill du delta i ett kommande revideringsarbete eller vara med och ta fram andra standarder inom området? Gå in på www.sis.se - där hittar du mer information.

Fastställd: 2023-08-14
ICS: 01.140.30; 03.100.70; 04.050; 33.040.40; 35.020; 35.030; 35.040; 35.080

Svenska Institutet för Standarder

Europastandarden EN ISO/IEC 27001:2023 gäller som svensk standard. Standarden fastställdes 2023-08-14 som SS-EN ISO/IEC 27001:2023 och har utgivits i den engelskspråkiga versionen. Detta dokument återger EN ISO/IEC 27001:2023 i svensk språkversion. De båda språkversionerna gäller parallellt.

Denna standard ersätter SS-EN ISO/IEC 27001:2017, utgåva 1 och SS-ISO/IEC 27001:2022, utgåva 3.

The European Standard EN ISO/IEC 27001:2023 has the status of a Swedish Standard. The standard was approved and published 2023-08-14 as SS-EN ISO/IEC 27001:2023 in English. This document contains a Swedish language version of EN ISO/IEC 27001:2023. The two versions are valid in parallel.

This standard supersedes the Swedish Standard SS-EN ISO/IEC 27001:2017, edition 1 and SS-ISO/IEC 27001:2022, edition 3.

Svenska Institutet för Standarder

LÄSANVISNINGAR FÖR STANDARDER

I dessa anvisningar behandlas huvudprinciperna för hur regler och yttre begränsningar anges i standardiseringsprodukter.

Krav
Ett krav är ett uttryck i ett dokuments innehåll som anger objektivt verifierbara kriterier som ska uppfyllas och från vilka ingen avvikelse tillåts om efterlevnad av dokumentet ska kunna åberopas. Krav uttrycks med hjälpverbet **ska** (eller **ska inte** för förbud).

Rekommendation
En rekommendation är ett uttryck i ett dokuments innehåll som anger en valmöjlighet eller ett tillvägagångssätt som bedöms vara särskilt lämpligt utan att nödvändigtvis nämna eller utesluta andra. Rekommendationer uttrycks med hjälpverbet **bör** (eller **bör inte** för avrådanden).

Instruktion
Instruktioner anges i imperativ form och används för att ange hur något görs eller utförs. De kan underordnas en annan regel, såsom ett krav eller en rekommendation. De kan även användas självständigt, och är då att betrakta som krav.

Förklaring
En förklaring är ett uttryck i ett dokuments innehåll som förmedlar information. En förklaring kan uttrycka tillåtelse, möjlighet eller förmåga. Tillåtelse uttrycks med hjälpverbet **får** (eller motsatsen **behöver inte**). Möjlighet och förmåga uttrycks med hjälpverbet **kan** (eller motsatsen **kan inte**).

READING INSTRUCTIONS FOR STANDARDS

These instructions cover the main principles for the use of provisions and external constraints in standardization deliverables.

Requirement
A requirement is an expression, in the content of a document, that conveys objectively verifiable criteria to be fulfilled, and from which no deviation is permitted if conformance with the document is to be claimed. Requirements are expressed by the auxiliary **shall** (or **shall not** for prohibition).

Recommendation
A recommendation is an expression, in the content of a document, that conveys a suggested possible choice or course of action deemed to be particularly suitable, without necessarily mentioning or excluding others. Recommendations are expressed by the auxiliary **should** (or **should not** for dissuasion).

Instruction
An instruction is expressed in the imperative mood and is used in order to convey an action to be performed. It can be subordinated to another provision, such as a requirement or a recommendation. It can also be used independently and is then to be regarded as a requirement.

Statement
A statement is an expression, in the content of a document, that conveys information. A statement can express permission, possibility or capability. Permission is expressed by the auxiliary **may** (its opposite being **need not**). Possibility and capability are expressed by the auxiliary **can** (its opposite being **cannot**).

EUROPASTANDARD
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 27001

Juli 2023

ICS 03.100.70; 35.030

Ersätter EN ISO/IEC 27001:2017

Svensk språkversion

Informationssäkerhet – Cybersäkerhet och integritetsskydd – Ledningssystem för informationssäkerhet – Krav (ISO/IEC 27001:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de management de la sécurité de l'information - Exigences (ISO/IEC 27001:2022)

Information security, cybersecurity and privacy protection - Information security management systems - Requirements (ISO/IEC 27001:2022)

Informationssicherheit, Cybersicherheit und Datenschutz - Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2022)

Denna Europastandard godkändes av CEN den 23 juli 2023.

CEN:s och Cenelecs medlemmar är skyldiga att följa CEN-Cenelecs interna bestämmelser där villkoren anges för att fastställa denna Europastandard som nationell standard utan ändringar. Aktuella förteckningar och litteraturhänvisningar som rör sådana nationella standarder kan beställas från CEN-Cenelecs centralsekretariat eller från CEN- och Cenelec-medlemmar .

Denna Europastandard finns i tre officiella versioner (engelsk, fransk och tysk). En version på något annat språk som översatts till en CEN-medlems eget språk, under dennes överinseende, och som anmälts till CEN-Cenelecs centralsekretariat, har samma status som de officiella versionerna.

CEN- och Cenelec-medlemmar är de nationella standardiseringsorganen och de nationella elektrotekniska kommittéerna i Belgien, Bulgarien, Cypern, Danmark, Estland, Finland, Frankrike, Grekland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Nederländerna, Nordmakedonien, Norge, Polen, Portugal, Rumänien, Schweiz, Serbien, Slovakien, Slovenien, Spanien, Storbritannien, Sverige, Tjeckien, Turkiet, Tyskland, Ungern och Österrike.

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

Innehållsförteckning

Sida

Förord

ISO (Internationella standardiseringsorganisationen) och IEC (Internationella elektrotekniska kommissionen) bildar ett speciellt system för internationell standardisering. Nationella organ som är medlemmar i ISO eller IEC deltar i utarbetandet av internationella standarder i tekniska kommittéer som har inrättats av respektive organisation för specifika tekniska verksamhetsområden. ISO:s och IEC:s tekniska kommittéer samarbetar inom områden av ömsesidigt intresse. Andra internationella organisationer, statliga såväl som icke-statliga, som samarbetar med ISO och IEC deltar också i arbetet.

De förfaranden som använts vid utarbetandet av det här dokumentet samt de som är avsedda att tillämpas vid uppdatering därav beskrivs i ISO/IEC-direktiven, del 1. Det bör särskilt noteras att det krävs olika godkännandekriterier för olika typer av dokument. Detta dokument har utarbetats i enlighet med de redaktionella reglerna i ISO/IEC-direktiven, del 2 (se www.iso.org/directives eller www.iec.ch/members_experts/refdocs).

Observera att vissa delar i detta dokument kan omfattas av patenträttigheter. ISO och IEC ansvarar inte i någon del för identifiering av sådana patenträttigheter. Information om eventuella patenträttigheter som identifierats under utarbetandet av dokumentet återges i avsnittet Inledning och/eller ISO:s förteckning över mottagna patentdeklarationer (se www.iso.org/patents) eller i IEC:s förteckning över mottagna patentdeklarationer (se patents.iec.ch).

Eventuella handelsnamn som förekommer i dokumentet anges som information för att underlätta för användarna och innebär inte något godkännande.

För förklarande information om standarders frivilliga karaktär, innebörden i ISO-specifika termer och uttryck som rör bedömning av överensstämmelse samt information om ISO:s efterlevnad av Världshandelsorganisationens (WTO:s) principer i avtalet om tekniska handelshinder (TBT) se www.iso.org/iso/foreword.html. För IEC, se www.iec.ch/understanding-standards.

Detta dokument har utarbetats av den gemensamma tekniska kommittén ISO/IEC JTC 1, *Information technology*, underkommitté SC 27, *Information security, cybersecurity and privacy protection*.

Denna tredje utgåva upphäver och ersätter den andra utgåvan (ISO/IEC 27001:2013), som har genomgått teknisk översyn. Den inbegriper även de tekniska rättelserna ISO/IEC 27001:2013/Cor 1:2014 och ISO/IEC 27001:2013/Cor 2:2015.

De huvudsakliga förändringarna i förhållande till den föregående utgåvan är:

– Texten har samordnats med den harmoniserade strukturen för standarder för ledningssystem och ISO/IEC 27002:2022.

Återkoppling eller frågor som rör det här dokumentet bör framföras till standardiseringsorganet i användarens land. En komplett förteckning över dessa organ finns på www.iso.org/members.html och www.iec.ch/national-committees.

Europeiskt förord

Texten i ISO/IEC 27001:2022 har utarbetats av den tekniska kommittén ISO/IEC JTC 1 ”Information technology” och har tagits över som EN ISO/IEC 27001:2023 av den tekniska kommittén CEN-CENELEC/JTC 13 ”Cybersecurity and Data Protection”, vars sekretariat innehas av DIN.

Denna Europastandard ska fastställas som nationell standard, antingen genom publicering av en identisk text eller genom ikraftsättning, senast januari 2024. Motstridande nationella standarder ska ha upphävts senast januari 2024.

Observera att vissa delar av detta dokument kan omfattas av patenträttigheter. CEN-Cenelec ansvarar inte i någon del för identifiering av sådana patenträttigheter.

Detta dokument ersätter EN ISO/IEC 27001:2017.

Eventuell återkoppling eller frågor som rör det här dokumentet bör framföras till standardiseringsorganet i användarens land. En komplett förteckning över dessa organ finns på CEN:s och Cenelecs webbplatser.

Enligt CEN-Cenelecs interna bestämmelser ska denna Europastandard fastställas av de nationella standardiseringsorganen i följande länder: Belgien, Bulgarien, Cypern, Danmark, Estland, Finland, Frankrike, Grekland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Nederländerna, Nordmakedonien, Norge, Polen, Portugal, Rumänien, Schweiz, Serbien, Slovakien, Slovenien, Spanien, Storbritannien, Sverige, Tjeckien, Turkiet, Tyskland, Ungern och Österrike.

Meddelande om ikraftsättning

Texten i ISO/IEC 27001:2022 har godkänts av CEN-Cenelec som EN ISO/IEC 27001:2023 utan någon ändring.

Inledning

0.1 Allmänt

Detta dokument har utarbetats i syfte att ange krav för att upprätta, införa, upprätthålla och ständigt förbättra ett ledningssystem för informationssäkerhet. Införandet av ett ledningssystem för informationssäkerhet är ett strategiskt beslut för en organisation. Upprättandet och införandet av en organisations ledningssystem för informationssäkerhet påverkas av organisationens behov och mål, säkerhetskrav, tillämpade organisationsprocesser samt organisationens storlek och struktur. Samtliga dessa påverkansfaktorer beräknas kunna förändras med tiden.

Ledningssystemet för informationssäkerhet upprätthåller informationens konfidentialitet, riktighet och tillgänglighet genom en riskhanteringsprocess och skapar förtroende hos intressenter att risker hanteras på lämpligt sätt.

Det är viktigt att ledningssystemet för informationssäkerhet utgör en integrerad del av organisationens processer och övergripande ledningsstruktur och att informationssäkerhet beaktas när processer, informationssystem och säkerhetsåtgärder utformas. Införandet av ett ledningssystem för informationssäkerhet förväntas komma att anpassas till organisationens behov.

Detta dokument kan användas av interna och externa parter för att bedöma organisationens förmåga att uppfylla organisationens egna informationssäkerhetskrav.

Presentationsordningen för dokumentets krav speglar inte deras betydelse och anger inte heller i vilken ordning de ska införas. Numreringen av listpunkter görs enbart i hänvisningssyfte.

I ISO/IEC 27000 ges en översikt över ledningssystemen för informationssäkerhet och deras terminologi, med hänvisning till familjen av standarder avseende ledningssystem för informationssäkerhet (inklusive ISO/IEC 27003[2], ISO/IEC 27004[3] och ISO/IEC 27005[4]), med relaterade termer och definitioner.

0.2 Kompatibilitet med andra standarder för ledningssystem

I detta dokument tillämpas den övergripande struktur samt identiska underavsnittsrubriker, identisk text, gemensamma termer och definitioner som fastställts i bilaga SL till ISO/IEC Directives, Part 1, Consolidated ISO Supplement, och därmed upprätthålls kompatibiliteten till andra standarder för ledningssystem för vilka bilaga SL har antagits.

Det gemensamma tillvägagångssätt som definieras i bilaga SL kommer att vara användbart för organisationer som väljer att driva ett enda ledningssystem som uppfyller kraven för två eller flera standarder för ledningssystem.

Informationssäkerhet, cybersäkerhet och integritetsskydd – Ledningssystem för informationssäkerhet – Krav

1 Omfattning

I detta dokument specificeras kraven för att upprätta, införa, upprätthålla och ständigt förbättra ett ledningssystem för informationssäkerhet med hänsyn till organisationens förutsättningar. Detta dokument innehåller även krav för att bedöma och behandla informationssäkerhetsrisker anpassat efter organisationens behov. Kraven i detta dokument är allmänna och är avsedda att kunna tillämpas på alla organisationer, oavsett typ, storlek eller karaktär. Det är inte tillåtet att exkludera något av kraven i avsnitt 4–10 när en organisation anger efterlevnad av detta dokument.

2 Normativa hänvisningar

Följande dokument hänvisas till i texten på så sätt att deras innehåll, helt eller delvis, utgör krav i detta dokument. För daterade hänvisningar gäller endast den angivna utgåvan. För odaterade hänvisningar gäller den senaste utgåvan av dokumentet (inklusive eventuella tillägg).

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*