

 **ISO /IEC 27001**

Information Security Management System



KiNS konferansen 24. mai 2023

Olve Svéen
CISO

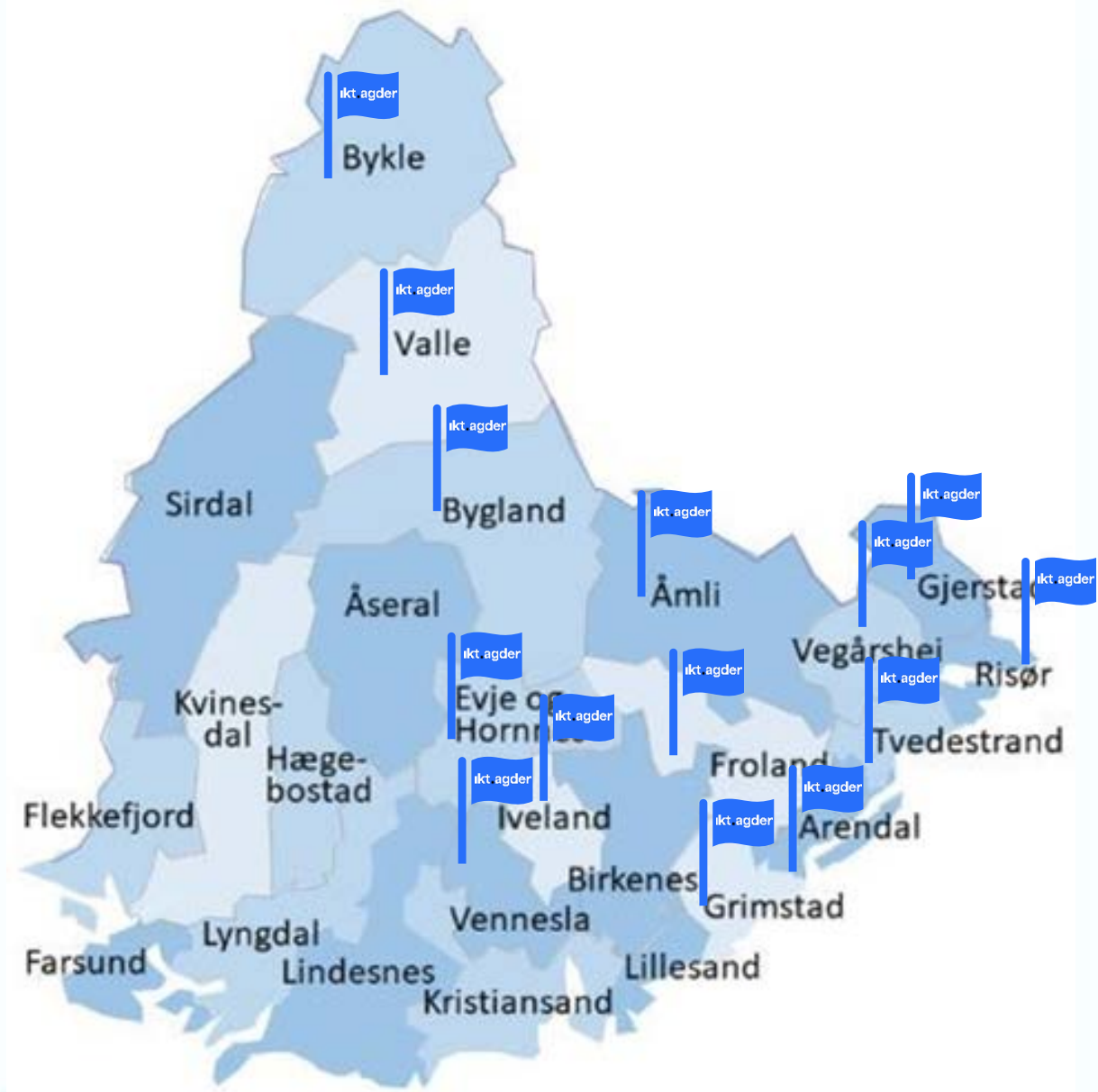
John A. Horve
Personvernombud

ikt.agder

Hvem er **ikt.agder**?

110 ansatte som betjener:

- 14 kommuner
- 1 fylkeskommune
- 11 kunder
- 30.000 PCer
- 7.000 nettbrett
- 47.000 brukere
- 16.000 ansatte



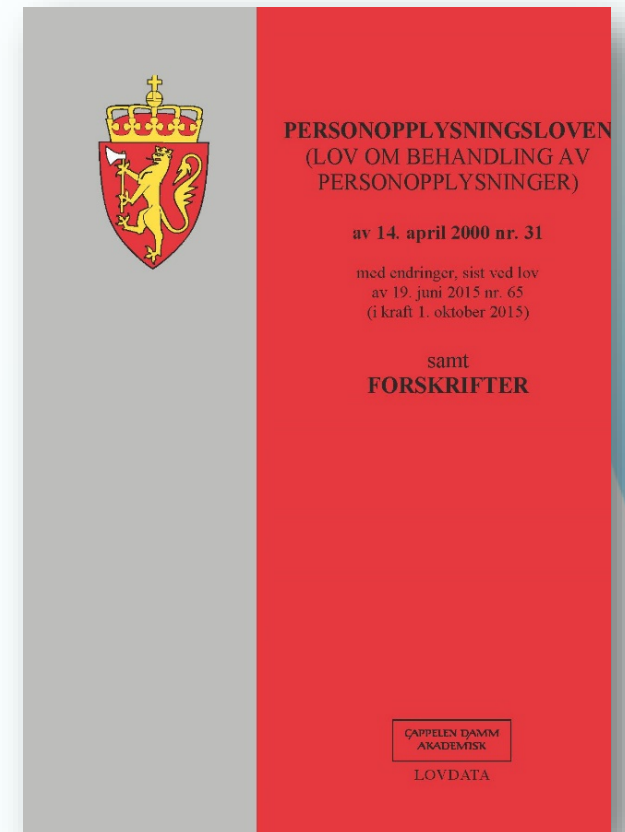
Krav i Personopplysningsforskriften fra 2001

§ 14. Internkontroll

Den behandlingsansvarlige skal **etablere og holde vedlike planlagte og systematiske tiltak** som er nødvendige for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes kvalitet.

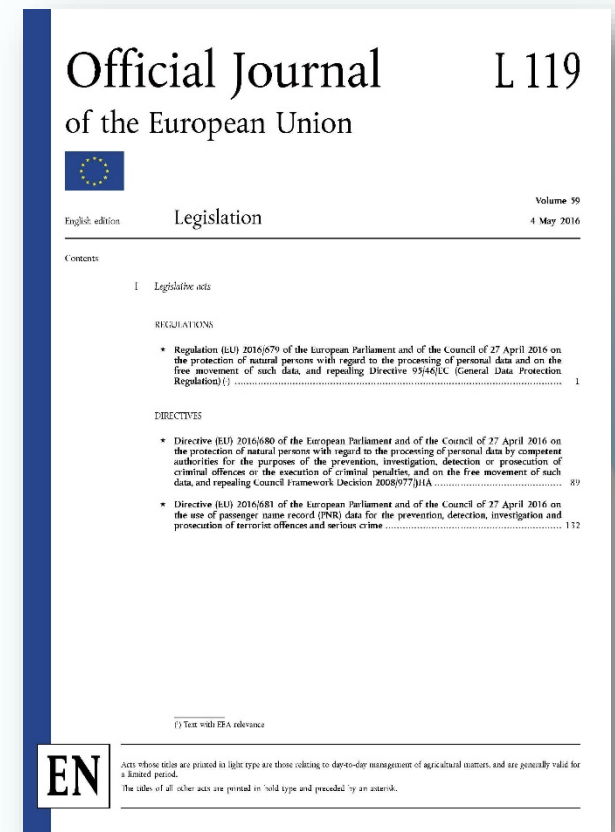
Den behandlingsansvarlige skal dokumentere tiltakene. **Dokumentasjonen skal være tilgjengelig for medarbeiderne** hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernemnda.

Kongen kan gi forskrift med nærmere regler om internkontroll.



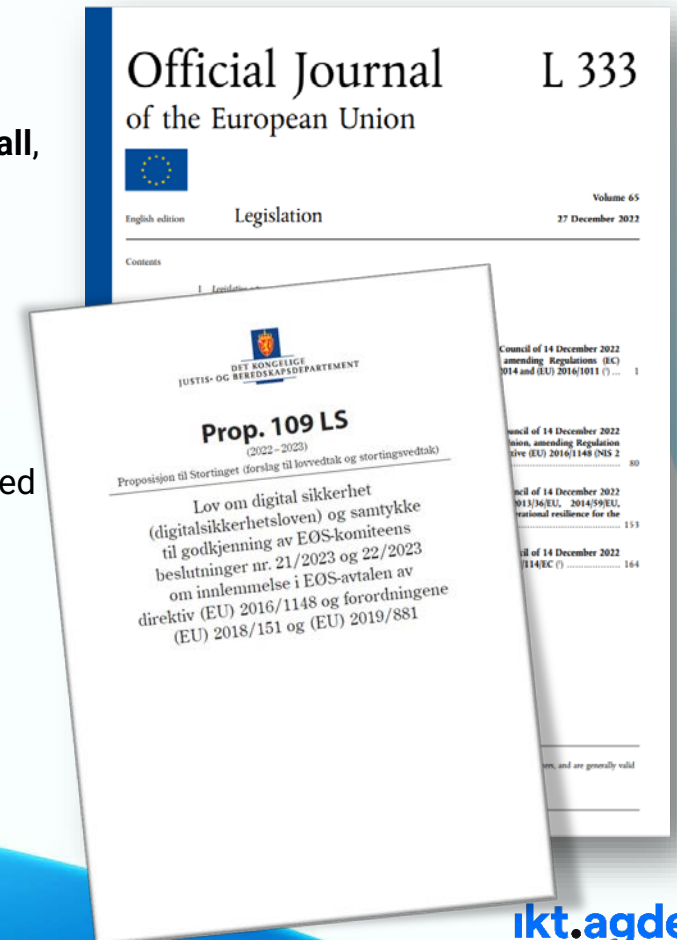
Artikkel 24 – Den behandlingsansvarliges ansvar

1. Idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige **gjennomføre egnede tekniske og organisatoriske tiltak** for å sikre og **påvise at behandlingen utføres i samsvar med denne forordning**. Nevnte tiltak **skal gjennomgås på nytt og skal oppdateres ved behov**.
2. Dersom det står i et rimelig forhold til behandlingsaktivitetene, skal tiltakene nevnt i nr. 1 omfatte den behandlingsansvarliges iverksetting av egnede retningslinjer for vern av personopplysninger.
3. Overholdelse av godkjente atferdsnormer som nevnt i artikkel 40 eller godkjente sertifiseringsmekanismer som nevnt i artikkel 42 kan brukes som en faktor for å påvise at den behandlingsansvarliges forpliktelser overholdes.



Article 25 – Standardisation

1. In order to promote the convergent implementation of Article 21(1) and (2), **Member States shall**, without imposing or discriminating in favour of the use of a particular type of technology, **encourage the use of European and international standards and technical specifications relevant to the security of network and information systems.**
2. ENISA, in cooperation with Member States, and, where appropriate, after consulting relevant stakeholders, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including national standards, which would allow for those areas to be covered



Krav i Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten

2.4 Styringssystem

Alle virksomheter skal ha et styringssystem for informasjonssikkerhet og personvern (internkontroll).

Med styringssystem menes formalisering av hvordan virksomheten planlegger, gjennomfører, evaluerer/kontrollerer og korrigerer etterlevelse av relevant regelverk, krav og avtaler.

...

Styringssystemet skal dokumenteres. Dokumenter angitt i styringssystemet skal holdes løpende oppdatert og arkiveres fra det tidspunktet dokumentet ble erstattet med en ny gjeldende versjon. Dette kan f.eks. være rutiner for sikkerhetsrevisjoner, risikovurderinger, driftsrutiner, avvik og hvordan de håndteres, ledelsens gjennomgang, databehandleravtaler mv.

...



§ 15. Internkontroll på informasjonssikkerhetsområdet

Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.

Forvaltningsorganet skal ha en internkontroll (styring og kontroll) **på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet.** Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. Det organet departementet peker ut skal gi anbefalinger på området.

Omfang og innretning på internkontrollen skal være tilpasset risiko.



Representantskapet i IKT Agder IKS



28. april 2023

Representantskapet i IKT Agder IKS har 28. april 2023 vedtatt følgende Deltakerstrategi

IKT AGDER DELTAGERSTRATEGI – STERKERE SAMMEN						
Visjon	Samarbeid for en enklere hverdag					
Strategisk retning	Gode og sikre digitale kommunale tjenester for innbyggere og arbeidsliv på Agder	Gode og brukervennlige digitale verktøy som sikrer effektiv ressursbruk	Et fremtidsrettet og attraktivt IKT samarbeid, som legger til rette for effektivisering og tjenesteutvikling		IKT Agder – vår felles IT avdeling	
Fokusområder	Innbyggeren i sentrum	Effektiv og sikker drift og forvaltning	Standardisering og fellesløsninger	Sikkerhet og beredskap	Tjenesteutvikling og innovasjon	Attraktivt teknologisk selskap
Mål Vi skal ...	• Levere enkle, heldigitale innbyggertjenester, tilgjengelig 24/7 • Tilby sømløse sammenhengende innbyggertjenester • Tilrettelegge for åpenhet og demokratiske prosesser • Tilgjengeliggjøre kommunale datasets	• Tilstrebe 100% opptid • Levere tilfredsstillende brukerstøtte • Tilby IKT-verktøy tilpasset en moderne og fleksibel arbeidshverdag • Tilrettelegge for god dialog og samhandling	• Tilstrebe flest mulig fellesløsninger og likhet i arbeidsprosesser og IKT-verktøy • Utnytte mulighetene i nasjonalt økosystem og være lojale til valgte nasjonale fellesløsninger og standarder • Ivareta felles innkjøp av teknologi og utnytte markedsmakten • Tilrettelegge for pilotering og skalering – utvalgte kommuner «går foran og drar lasset» på vegne av fellesskapet • Tilrettelegge for valgfrihet innenfor gitte rammer	• Sikre et kommunalt systemer og data er tilfredsstillende beskyttet mot cyberangrep • Sørge for tilfredsstillende informasjons sikkerhet i kommunale IKT-systemer og data • Ivareta rollen som databehandler, og bistå deltagerne i sin rolle som behandlingsansvarlig • Pådriver for god sikkerhetskultur • Sikre god beredskap og tiltak mot uønskede hendelser	• Levere løsninger med høy brukervennlighet • Proaktiv utviklingspartner i tjenesteutvikling og digitalisering • Pådriver for at utviklingen er i tråd med fremtidens teknologiske trender • Delta i valgte nasjonale digitale initiativ • Tilrettelegge for innhenting, sammenstilling og analyse av data for å levere bedre tjenester • Stjele med stil og dele med glede	• Være det foretrukne alternativet for alle kommuner på Agder • Tilby et attraktivt kompetansemiljø • Ha en attraktiv arbeidsplass • Være en attraktiv og synlig samarbeidspartner for akademia og arbeidsliv • Forbli en attraktiv lærebedrift som bidrar til å sikre god opplæring
Vi har lykket når ...	• Vi er best i Agder og fremst i landet på digitale innbyggertjenester • Alle åpne kommunale datasets er tilgjengeliggjort • Det er høy tilfredshet hos innbyggerne, frivillige og arbeidsliv med våre digitale tjenester • Våre beslutningsprosesser er datarevne og autonome	• Vi leverer innenfor avtalt SLA på alle områder • Vi har god brukertilfredshet, med en jevn økning • 95 % av fellesprosjektene leveres innenfor toleransene • Vi har endret fokus fra fagsystem til helhetlig tjenesteutvikling • Kostnads- og prognosemodellen er tilgjengelig i sanntid	• Alle løsningene er en del av tjenestekatalogen • Vi har fått kostnadsoptimalt drift og forvaltning gjennom få ulike tjenester og dupliserte løsninger • Vi har fortløpende i bruk valgte nasjonale løsninger og data • Tjenestekatalogen er kjent og brukes som et verktøy i hverdagen • Vi har årlige beredskaps- og sikkerhetstester hos minimum 25% av deltakerne	• Vi har skapt en sterk sikkerhetskultur og sikkerheten er på ISO 27000 nivå • Vi har ingen sikkerhetsavvik eller nedetid på kritisk infrastruktur • ROS for selskapet, alle systemer og tjenester er til enhver tid oppdatert • Vi har årlige beredskaps- og sikkerhetstester hos minimum 25% av deltakerne	• Vi er en nasjonal aktør innenfor tjenesteutvikling og innovasjon • Vi samarbeider om å gjennomføre digital tjenesteutvikling effektivt • Tjenesteutviklingskjør innenfor et etablert og forankret teknisk mål bilde • Vi har utmerket oss i konkurranse om innovasjons- eller digitaliseringspris • Vi har høy digital modenhet, tilsvarende generasjon 4 nivå	• Selskapet har en sunn turnover og rekrutterer og beholder riktig kompetanse • Vi er en sentral bidragsyter for nasjonal kompetanseutvikling i tett samarbeid med akademia • Vi har utmerket oss med vår satsing på lærlinger og kompetanseutvikling

- Vi har skapt en sterk sikkerhetskultur og sikkerheten er på ISO 27000 nivå
- Vi har ingen sikkerhetsavvik eller nedetid på kritisk infrastruktur
- ROS for selskapet, alle systemer og tjenester er til enhver tid oppdatert
- Vi har årlige beredskaps- og sikkerhetstester hos minimum 25% av deltakerne

Sikkerhetshåndbok

- Styrende del
- Gjennomførende del
- Kontrollerende del
- Løpende revidering



2019

Innstilling om å etablere et mer standardisert ISMS

2020

Anskaffet Neupart som verktøy for ISMS

2021

Innstilling om prosjekt for ISMS iht ISO 27001

2022

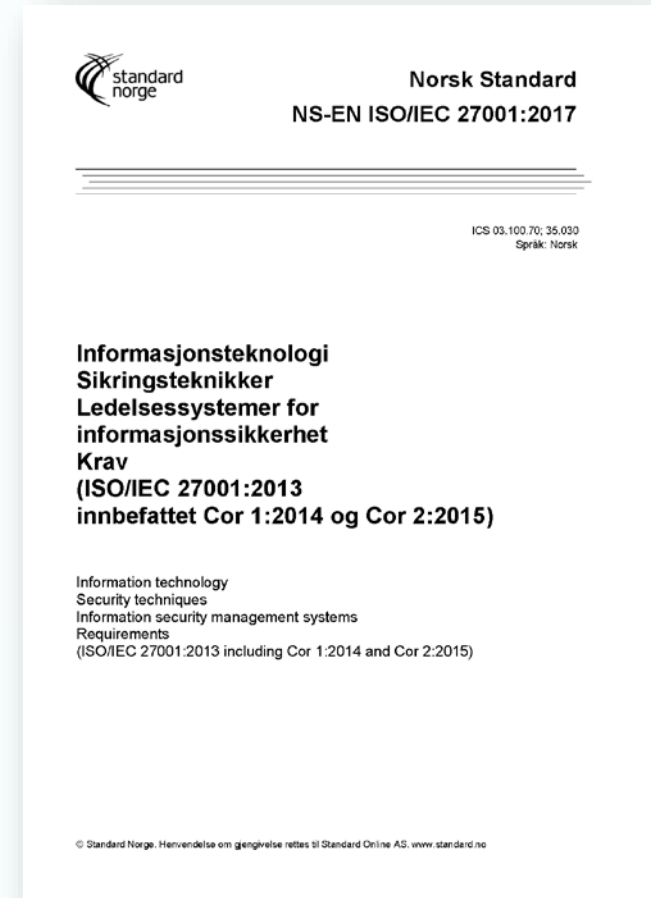
Formell oppstart av prosjekt for ISMS



Dette er  / IEC 27001

Områder i standarden

4. Organisasjonens kontekst
5. Lederskap
6. Planlegging
7. Støtte
8. Drift
9. Prestasjonsevaluering
10. Forbedring





1. Identifisere og kartlegge

1.1 Kartlegg styringsstrukturer, leveranser og understøttende systemer

1.2 Kartlegg enheter og programvare

1.3 Kartlegg brukere og behov for tilgang



2. Beskytte og opprettholde

2.1 Ivareta sikkerhet i anskaffelses- og utviklingsprosesser

2.3 Ivareta en sikker konfigurasjon

2.5 Kontroller dataflyt

2.7 Beskytt data i ro og i transitt

2.9 Etabler evne til gjenoppretting av data

2.2 Etabler en sikker IKT-arkitektur

2.4 Beskytt virksomhetens nettverk

2.6 Ha kontroll på identiteter og tilganger

2.8 Beskytt e-post og nettleser

2.10 Integrer sikkerhet i prosess for endringshåndtering



3. Oppdage

3.1 Oppdag og fjern kjente sårbarheter og trusler

3.2 Etabler sikkerhets- overvåkning

3.3 Analyser data fra sikkerhets- overvåkning

3.4 Gjennomfør inntrengings- tester



4. Håndtere og gjenopprette

4.1 Forbered virksomheten på håndtering av hendelser

4.2 Vurder og klassifiser hendelser

4.3 Kontroller og håndter hendelser

4.4 Evaluer og lær av hendelser

NSMs grunnprinsipper mappet mot ISO 27002

NSMs grunnprinsipper for IKT-sikkerhet v2.0									Kobling mellom NSM GP-IKT 2.0 og ISO/IEC 27002:2013													
Nr.	Kategori	GP. ID	Grunnprinsipp	Spesifisering	Tiltak ID	Tiltaksoverskrift	Tiltaksbeskrivelse	Prioritet	A	B	C	D	E	F	G	H	I	J	K	L	M	N
67	Beskytte og opprettholde	2.8	Beskytt e-post og nettleser	Implementering av dette applikasjonsspesifikke prinsippet anbefales utført etter andre tiltak, se informasjon etter tabellen.	2.8.3	Bruk kun støttede e-postklienter, nettlesere og programtillegg	Bruk kun støttede e-postklienter, nettlesere og programtillegg («plugins») i virksomheten. Bruk kun siste versjoner med den nyeste sikkerhetsfunksjonaliteten og de siste sikkerhetsoppdateringene. Avinstaller/deaktiver nettlesere som er inkludert i operativsystemet og som ikke lenger støttes.	3	A.14.1.1													
68	Beskytte og opprettholde	2.8	Beskytt e-post og nettleser	Implementering av dette applikasjonsspesifikke prinsippet anbefales utført etter andre tiltak, se informasjon etter tabellen.	2.8.4	Tillat kun virksomhetsgodkjente programtillegg	Tillat kun virksomhetsgodkjente programtillegg. For mange virksomheter er nødvendige programtillegg («plugins») kun de som integrerer epostleser og nettleser mot for eksempel søk og arkivsystemer. Tillegg som ikke er nødvendige for virksomheten kan utgjøre en sårbarhet, og bør derfor ikke tillates.	2	A.14.1.1													
69	Beskytte og opprettholde	2.9	Etabler evne til gjenoppretting av data		2.9.1	Legg en plan for regelmessig sikkerhetskopiering av alle virksomhetsdata	Legg en plan for regelmessig sikkerhetskopiering av alle virksomhetsdata. En slik plan bør som minimum beskrive: a) Hvilke data som skal sikkerhetskopieres. b) Regelmessighet på sikkerhetskopiering av ulike data, basert på verdi. c) Ansvar for sikkerhetskopiering av ulike data. d) Prosedyrer ved feilet sikkerhetskopiering. e) Oppbevaringsperiode for sikkerhetskopier. f) Logiske og fysiske krav til sikring av sikkerhetskopier. g) Krav til gjenopprettingstid for virksomhetens ulike systemer og data (se prinsipp 4.1 - Forbered virksomheten på hendelser). h) Godkjenningssansvar/diagram for planen.	1	A.12.3.1													
70	Beskytte og opprettholde	2.9	Etabler evne til gjenoppretting av data		2.9.2	Inkluder sikkerhetskopier av programvare	Inkluder sikkerhetskopier av programvare for å sikre gjenoppretting. Dette inkluderer (som minimum) a) sikkerhetskopiering av ref. prinsipp 2.3 - Ivarsette en sikker konfigurasjon og b) maler for virtuelle maskiner og «master-images» av operativsystemer og c) maler for virtuelle maskiner og «master-images» av operativsystemer og c)	3	A.12.3.1													
71	Beskytte og opprettholde	2.9	Etabler evne til gjenoppretting av data		2.9.3	Test sikkerhetskopier regelmessig	Test sikkerhetskopier regelmessig ved å utføre gjenopprettingstest for å verifisere at sikkerhetskopien fungerer.	2	A.12.3.1													
72	Beskytte og opprettholde	2.9	Etabler evne til gjenoppretting av data		2.9.4	Beskytt sikkerhetskopier mot tilsikt og utilsiktet sletting, manipulering og avlesning	Beskytt sikkerhetskopier mot tilsikt og utilsiktet sletting, manipulering og avlesning. a) Sikkerhetskopier bør være separert fra virksomhetens produksjonsmiljø. Se bl.a. prinsipp 2.1 - Ivarsette sikkerhet i anskaffelses- og utviklingsprosesser. b) Tilgangstilhørigheter til sikkerhetskopier bør begrenses til kun ansatte og systemprosesser som skal gjenopprette data. c) Det bør jevnlig tas offline sikkerhetskopier som ikke kan nås via virksomhetens nettverk. Dette for å hindre tilsikt/ utilsiktet sletting eller manipulering. d) Sikkerhetskopier bør beskyttes med kryptering, nåddetilgang eller flyttes over nettverket. Dette inkluderer ...	3	A.12.3.1													
73	Beskytte og opprettholde	2.10	Integrer sikkerhet i prosess for endringshåndtering		2.10.1	Integrer sikkerhet i virksomhetens prosess for endringshåndtering	Integrer sikkerhet i virksomhetens prosess for endringshåndtering. Prosess for endringshåndtering bør inkludere: a) Vurdering av endringsforslag for å identifisere påvirkning på etablerte sikkerhetstiltak, f.eks. tiltakene som er beskrevet i alle tabellene i grunnprinsipper for IKT-sikkerhet. b) Krav til testing av endringer før og etter idriftsetting, se prinsipp 2.1 - Ivarsette sikkerhet i anskaffelses- og utviklingsprosesser. c) Informasjon til og nødvendig involvering av interessenter som blir påvirket av endringen. d) Dokumentering av vurderinger, anbefalinger, avgjørelser og gjennomganger/tester med relevans for	3	A.12.1.2	A.12.5.1	A.14.2.2	A.14.2.3	A.14.2.5									
74	Beskytte og opprettholde	2.10	Integrer sikkerhet i prosess for endringshåndtering		2.10.2	Involver nødvendig IKT-sikkerhetspersonell i forbindelse med endringer	Involver nødvendig IKT-sikkerhetspersonell i forbindelse med endringer. Det kan være i forbindelse med overordnede eller tekniske vurderinger og gjennomganger, testing, godkjenning/signering eller varsling.	2	A.12.1.2	A.14.2.2												
75	Beskytte og opprettholde	2.10	Integrer sikkerhet i prosess for endringshåndtering		2.10.3	Gjennomfør nødvendig endring, konfigurering og testing av påvirkede sikkerhetsfunksjoner	Gjennomfør nødvendig endring, konfigurering og testing av påvirkede sikkerhetsfunksjoner før og etter idriftsetting for å opprettholde etablert sikkerhetstilstand.	3	A.12.1.2	A.12.5.1	A.14.2.2	A.14.2.3										
76	Beskytte og opprettholde	2.10	Integrer sikkerhet i prosess for endringshåndtering		2.10.4	Integrer sikkerhet i virksomhetens prosess for hasterendringer	Integrer sikkerhet i virksomhetens prosess for hasterendringer. Fastsett minimumskrav til involvering av personell, sikkerhetsvurderinger, testing og dokumentasjon både før og etter idriftsetning, se 2.10.1 - 2.10.3.	3	A.12.1.2													
77	Oppdage	3.1	Oppdag og fjern kjente sårbarheter og trusler		3.1.1	Gjennomfør jevnlig sårbarhetskartlegging	Gjennomfør jevnlig sårbarhetskartlegging i informasjonssystemet ved hjelp av automatiserte verktøy. Kartleggingen bør dekke klienter, servere og nettverk. a) Prioriter funn og verifiser at oppdagede sårbarheter blir håndtert. b) Sørg for at verktøy benyttet til sårbarhetskartlegging jevnlig blir oppdatert med informasjon om alle relevante sikkerhetssårbarheter.	2	A.12.2.1	A.12.6.1	A.18.2.3											
78	Oppdage	3.1	Oppdag og fjern kjente sårbarheter og trusler		3.1.2	Abonner på tjenester relatert til sårbarhetsetterretning	Abonner på tjenester relatert til sårbarhetsetterretning for å være oppdatert på nye og kommende sårbarheter. Bruk denne informasjonen som input til verktøyene for	3	A.12.2.1	A.12.6.1												
79	Oppdage	3.1	Oppdag og fjern kjente sårbarheter og trusler		3.1.3	Benytt automatisert og sentralisert verktøy for å håndtere kjente trusler (som skadevare)	Benytt automatisert og sentralisert verktøy for å håndtere kjente trusler (som skadevare). a) Bruk antivirus/antiskadevare, fortrinnsvis en sentralisert styrt løsning, for å oppdage og blokkere kjent skadevare som blant annet utnytter sårbarheter i e-postklienter og dokumentlesere. b) Benytt også IDS/IPS-funksjonalitet på klienter og servere. c) Hendelser fra disse verktøyene bør løses, se prinsipp 3.2 - Etabler sikkerhetsovervåkning.	2	A.12.2.1	A.12.6.1												



NASJONAL SIKKERHETSMYNDIGHET

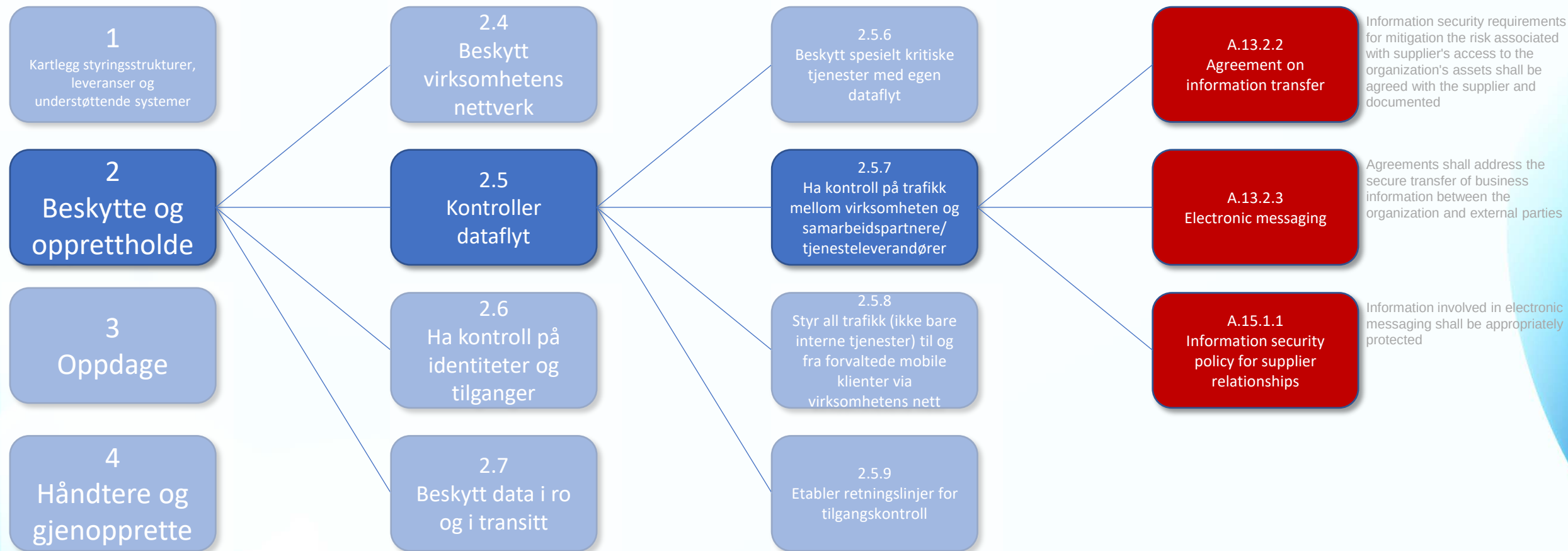


Kategori

Prinsipp

Tiltak

ISO/IEC 27001 Appendix A



Viktig med et dokumenthåndteringsverktøy

Ved å samle all dokumentasjon i ett verktøy forenkler det tilsyn og revisjon



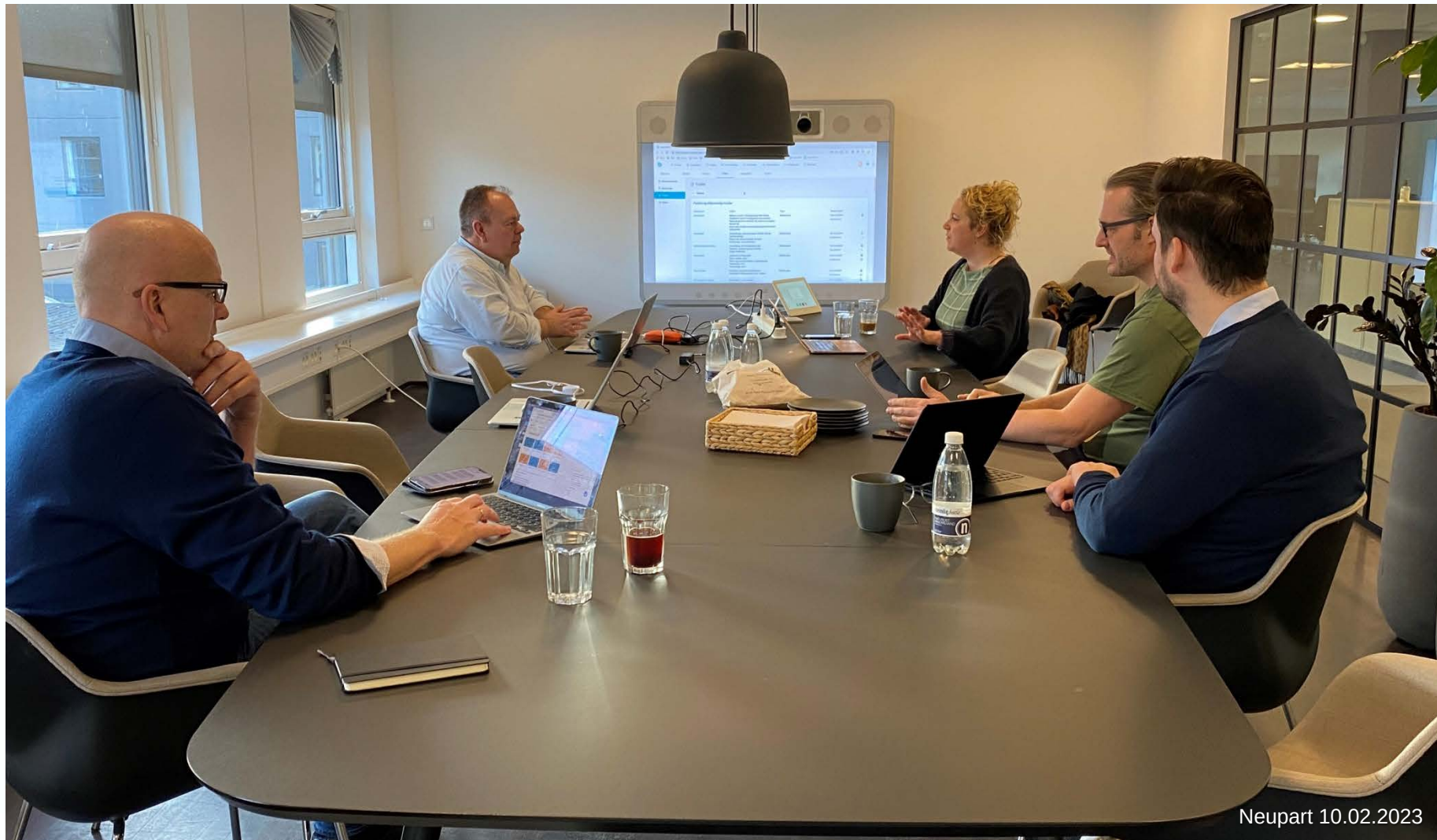
ISO/IEC 27701
Privacy Information
Management System



ISO/IEC 27001
Information Security
Management System



Besøk hos  neupart



Neupart 10.02.2023

Toppledelsen i selskapet – har sine egne tanker om hvordan bygge opp til en bra fest



Viktig med ledelsesforankring

ikt.agder

Agenda fagdag

Kl. 10:00- 10:30: Innledning v/ Daglig leder Rune Johansen og miljøgruppa

Kl. 15:45: Takk for i dag, avslutning med informasjon om kveldens julebord

Enklere hverdag

Fagdag for IKT Agder 25. november 2022

ikt.agder



Nye kontroller i 2022 versjonen

5.7 Trusseletterretning

5.23 Informasjonssikkerhet for bruk av skytjenester

5.30 IKT-beredskap for forretningskontinuitet

7.4 Fysisk sikkerhetsovervåking

8.9 Konfigurasjonsadministrasjon

8.10 Informasjonssletting

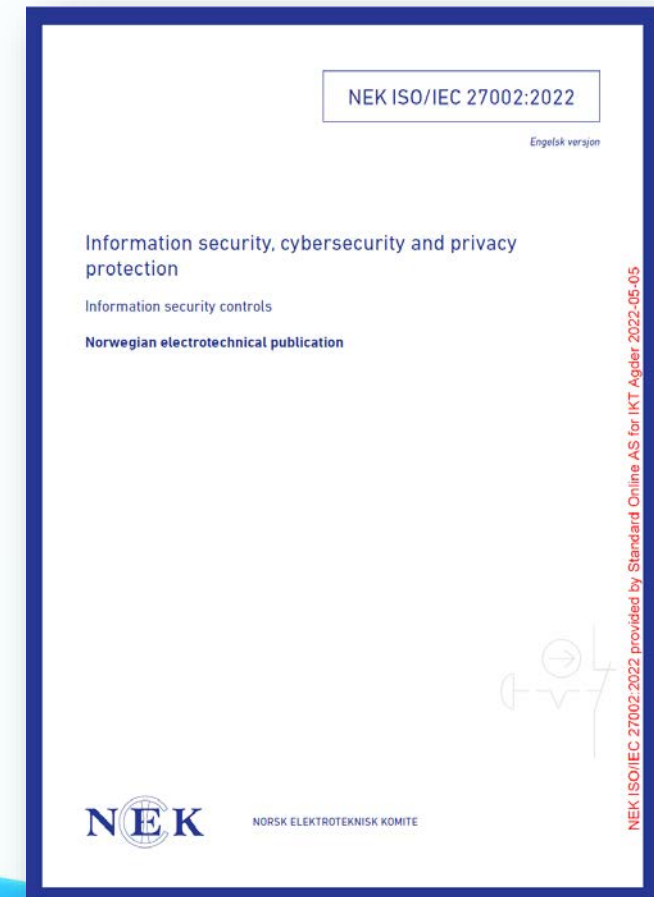
8.11 Datamaskering

8.12 Forebygging av datalekkasje

8.16 Overvåkingsaktiviteter

8.23 Nettfiltrering

8.28 Sikker koding



Organisatoriske sikkerhetstiltak

- 5.1 Policyer for informasjonssikkerhet
- 5.2 Roller og ansvar for informasjonssikkerhet
- 5.3 Arbeidsdeling
- 5.4 Ledelsesansvar
- 5.5 Kontakt med myndigheter
- 5.6 Kontakt med spesielle interessegrupper
- 5.7 Trusseletterretning
- 5.8 Informasjonssikkerhet i prosjektstyring
- 5.9 Oversikt over informasjonsverdier og andre tilknyttede verdier
- 5.10 Akseptabel bruk av informasjonsverdier og tilknyttede verdier
- 5.11 Retur av verdier
- 5.12 Klassifisering av informasjon
- 5.13 Merking av informasjon
- 5.14 Informasjonsoverføring
- 5.15 Tilgangskontroll
- 5.16 Identitetshåndtering
- 5.17 Autentiseringsinformasjon
- 5.18 Tilgangsrettigheter
- 5.19 Informasjonssikkerhet i leverandørforhold
- 5.20 Håndtering av informasjonssikkerhet i leverandøravtaler
- 5.21 Håndtering av informasjonssikkerhet i IKT-leveransekjeden
- 5.22 Overvåking, gjennomgang og endringshåndtering av leverandørtjenester
- 5.23 Informasjonssikkerhet ved bruk av skytjenester
- 5.24 Planlegging og forberedelse for håndtering av informasjonssikkerhetshendelser
- 5.25 Behandling av informasjonssikkerhetsepisoder
- 5.26 Respons på informasjonssikkerhetshendelser
- 5.27 Læring av informasjonssikkerhetshendelser
- 5.28 Innsamling av bevis
- 5.29 Informasjonssikkerhet under forstyrrelser
- 5.30 IKT-beredskap for virksomhetskontinuitet
- 5.31 Juridiske, lovfestede, regulatoriske og kontraktsmessige krav
- 5.32 Immaterielle rettigheter
- 5.33 Beskyttelse av virksomhetsdokumentasjon
- 5.34 Personvern og beskyttelse av PII
- 5.35 Uavhengig gjennomgang av informasjonssikkerhet
- 5.36 Samsvar med policyer, regler og standarder for informasjonssikkerhet
- 5.37 Dokumenterte driftsprosedyrer

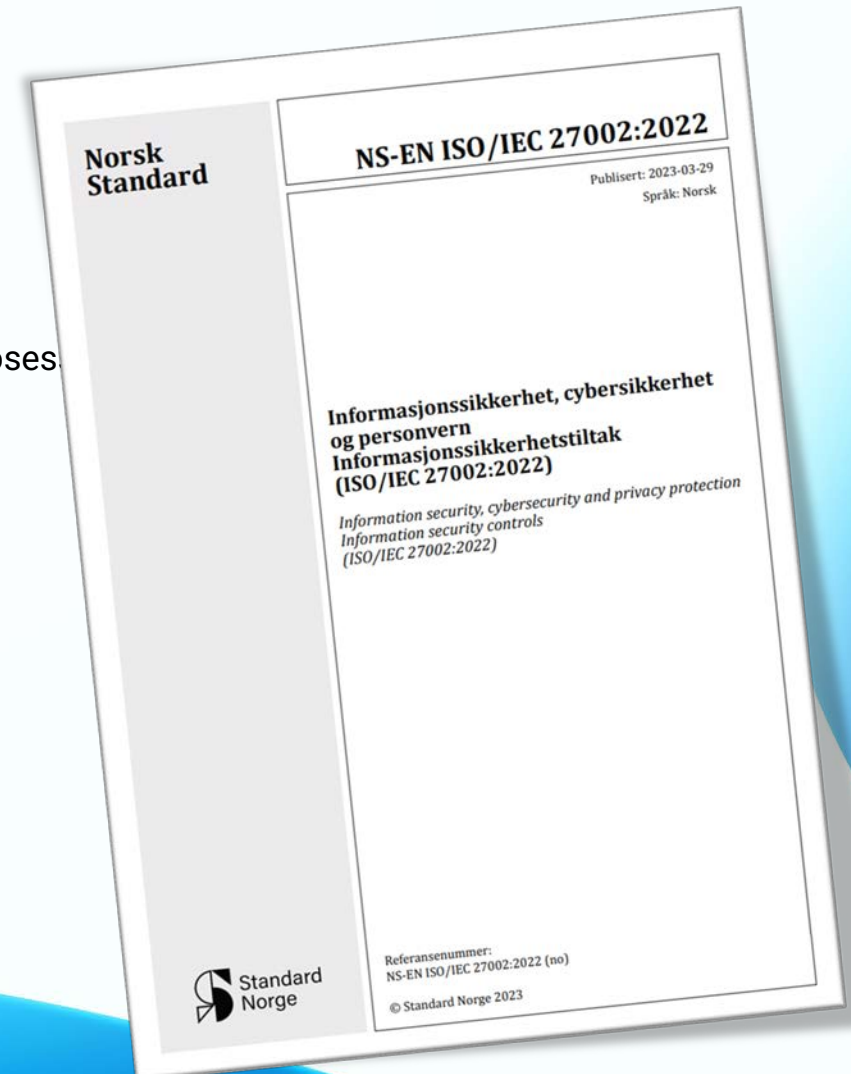
5.17 Autentiseringsinformasjon

Sikkerhetstiltak

Tildeling og administrasjon av autentiseringsinformasjon bør være underlagt en styringsprosess som inkluderer det å gi råd til personell om riktig håndtering av autentiseringsinformasjon.

Formål

Å sikre riktig entitetsautentisering og forhindre feil i autentiseringsprosesser.

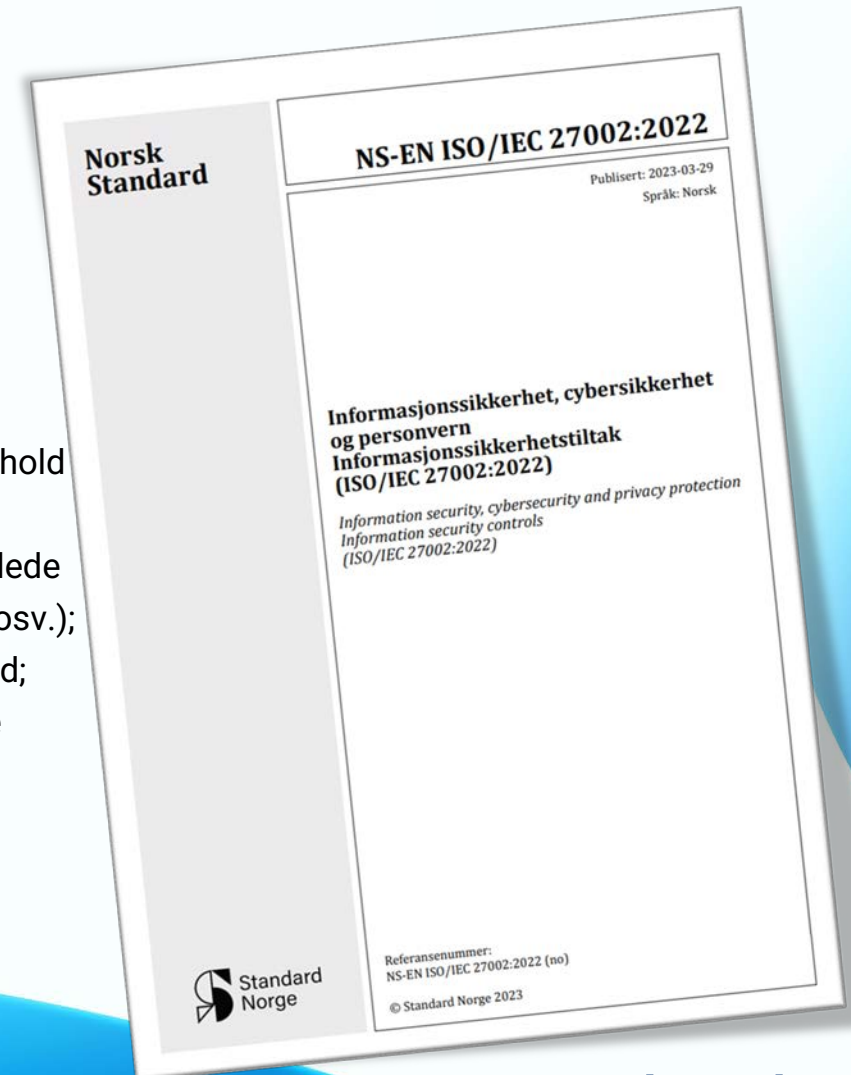


5.17 Autentiseringsinformasjon – veiledning

Brukeransvar

Alle som har tilgang til eller bruker autentiseringsinformasjon, bør rådes til å sikre:

- c) at det, når passord brukes som autentiseringsinformasjon, velges sterke passord i henhold anbefalt beste praksis, f.eks.:
 - 1) at passord ikke skal være basert på noe en annen person enkelt kan gjette eller utlede ved hjelp av personrelatert informasjon (f.eks. navn, telefonnumre, fødselsdatoer osv.);
 - 2) at passord ikke skal være basert på ordboksord eller på kombinasjoner av slike ord;
 - 3) at det brukes passordsetninger som er enkle å huske, som helst også bør omfatte alfanumeriske tegn og spesialtegn;
 - 4) at passordene har en minimumslengde;



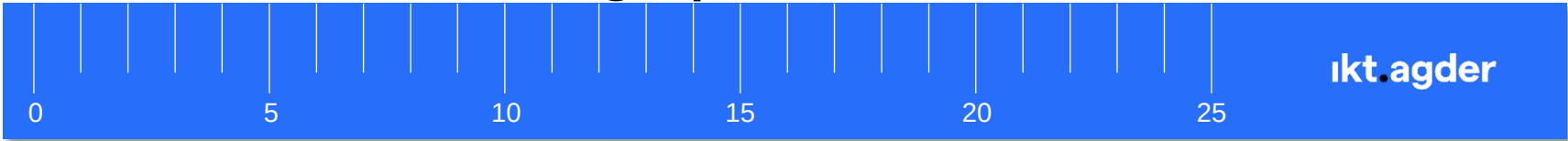
Passord sin styrke

Antall tegn	Bare tall	Små bokstaver	Store og små bokstaver	Tall, små og store bokstaver	Tall, små og store bokstaver og symboler
4	Umiddelbart	Umiddelbart	Umiddelbart	Umiddelbart	Umiddelbart
5	Umiddelbart	Umiddelbart	Umiddelbart	Umiddelbart	Umiddelbart
6	Umiddelbart	Umiddelbart	Umiddelbart	1 sekund	5 sekunder
7	Umiddelbart	Umiddelbart	25 sekunder	1 minutt	6 minutter
8	Umiddelbart	5 sekunder	22 minutter	1 time	8 timer
9	Umiddelbart	2 minutter	19 timer	3 dager	3 uker
10	Umiddelbart	58 minutter	1 måned	7 måneder	5 år
11	2 sekunder	1 dag	5 år	41 år	400 år
12	25 sekunder	3 uker	300 år	2.000 år	34.000 år
13	4 minutter	1 år	16.000 år	100.000 år	2.000.000 år
14	41 minutter	51 år	800.000 år	9.000.000 år	200.000.000 år
15	6 timer	1.000 år	43.000.000 år	600.000.000 år	15.000.000.000 år
16	2 dager	34.000 år	2.000.000.000 år	37.000.000.000 år	1.000.000.000.000 år
17	4 uker	800.000 år	100.000.000.000 år	2.000.000.000.000 år	93.000.000.000.000 år
18	9 måneder	23 millioner år	6.000.000.000.000 år	100.000.000.000.000 år	7.000.000.000.000.000 år

Kilde: <https://www.hivesystems.io>

Er det mulig å huske et langt passord?

olvelikerlangepassord



Passord sin styrke

Antall tegn	Bare tall	Små bokstaver	Store og små bokstaver	Tall, små og store bokstaver	Tall, små og store bokstaver og symboler
4	Umiddelbart	Umiddelbart	Umiddelbart	Umiddelbart	Umiddelbart
5	Umiddelbart	Umiddelbart	Umiddelbart	Umiddelbart	Umiddelbart
6	Umiddelbart	Umiddelbart	Umiddelbart	1 sekund	5 sekunder
7	Umiddelbart	Umiddelbart	25 sekunder	1 minutt	6 minutter
8	Umiddelbart	5 sekunder	22 minutter	1 time	8 timer
9	Umiddelbart	2 minutter	19 timer	3 dager	3 uker
10	Umiddelbart	58 minutter	1 måned	7 måneder	5 år
11	2 sekunder	1 dag	5 år	41 år	400 år
12	25 sekunder	3 uker	300 år	2.000 år	34.000 år
13	4 minutter	1 år	16.000 år	100.000 år	2.000.000 år
14	41 minutter	51 år	800.000 år	9.000.000 år	200.000.000 år
15	6 timer	1.000 år	43.000.000 år	600.000.000 år	15.000.000.000 år
16	2 dager	34.000 år	2.000.000.000 år	37.000.000.000 år	1.000.000.000.000 år
17	4 uker	800.000 år	100.000.000.000 år	2.000.000.000.000 år	93.000.000.000.000 år
18	9 måneder	23 millioner år	6.000.000.000.000 år	100.000.000.000.000 år	7.000.000.000.000.000 år

iktagder

Personellrelaterte sikkerhetstiltak

- 6.1 Bakgrunnssjekk
- 6.2 Vilkår og betingelser for ansettelse
- 6.3 Bevisstgjøring, utdanning og opplæring i informasjonssikkerhet
- 6.4 Disiplinærprosess
- 6.5 Ansvar etter opphør eller endring av ansettelsesforhold
- 6.6 Konfidensialitets- eller taushetserklæringer
- 6.7 Fjernarbeid
- 6.8 Rapportering av informasjonssikkerhetsepisoder

Fysiske sikkerhetstiltak

- 7.1 Fysiske sikkerhetssoner
- 7.2 Fysisk adgang
- 7.3 Sikring av kontorer, rom og fasiliteter
- 7.4 Fysisk sikkerhetsovervåkning
- 7.5 Beskyttelse mot fysiske og miljømessige trusler
- 7.6 Arbeid i sikre områder
- 7.7 Ryddig arbeidsplass og låst skjerm
- 7.8 Plassering og beskyttelse av utstyr
- 7.9 Sikring av verdier utenfor organisasjonens fysiske lokasjon
- 7.10 Lagringsmedier
- 7.11 Understøttende forsyningssystemer
- 7.12 Kablingssikkerhet
- 7.13 Vedlikehold av utstyr
- 7.14 Sikker avhending eller gjenbruk av utstyr

Teknologiske sikkerhetstiltak

- 8.1 Sluttbrukerenheter
- 8.2 Privilegerte tilgangsrettigheter
- 8.3 Begrensninger på informasjonstilgang
- 8.4 Tilgang til kildekode
- 8.5 Sikker autentisering
- 8.6 Kapasitetsstyring
- 8.7 Beskyttelse mot skadevare
- 8.8 Håndtering av tekniske sårbarheter
- 8.9 Konfigurasjonsstyring
- 8.10 Sletting av informasjon
- 8.11 Datamaskering
- 8.12 Forebygging av datalekkasje
- 8.13 Sikkerhetskopiering av informasjon
- 8.14 Redundans for fasiliteter for informasjonsbehandling
- 8.15 Logging
- 8.16 Overvåkningsaktiviteter
- 8.17 Klokkesynkronisering
- 8.18 Bruk av privilegerte hjelpeprogrammer
- 8.19 Installasjon av programvare i operative systemer
- 8.20 Nettverkssikkerhet
- 8.21 Sikring av nettverkstjenester
- 8.22 Segregering av nettverk
- 8.23 Nettstedfiltrering
- 8.24 Bruk av kryptografi
- 8.25 Sikkert utviklingslivsløp
- 8.26 Krav til applikasjonssikkerhet
- 8.27 Prinsipper for sikker systemarkitektur og prosjektering av sikre systemer
- 8.28 Sikker koding
- 8.29 Sikkerhetstesting i utvikling og akseptanse
- 8.30 Utkontraktet utvikling
- 8.31 Separasjon av utviklings-, test- og produksjonsmiljøer
- 8.32 Endringshåndtering
- 8.33 Testinformasjon
- 8.34 Beskyttelse av informasjonssystemer under revisjonstesting

8.15 Logging

Sikkerhetstiltak

Logger som registrerer aktiviteter, avvik, feil og andre relevante hendelser, bør produseres, oppbevares, beskyttes og analyseres.

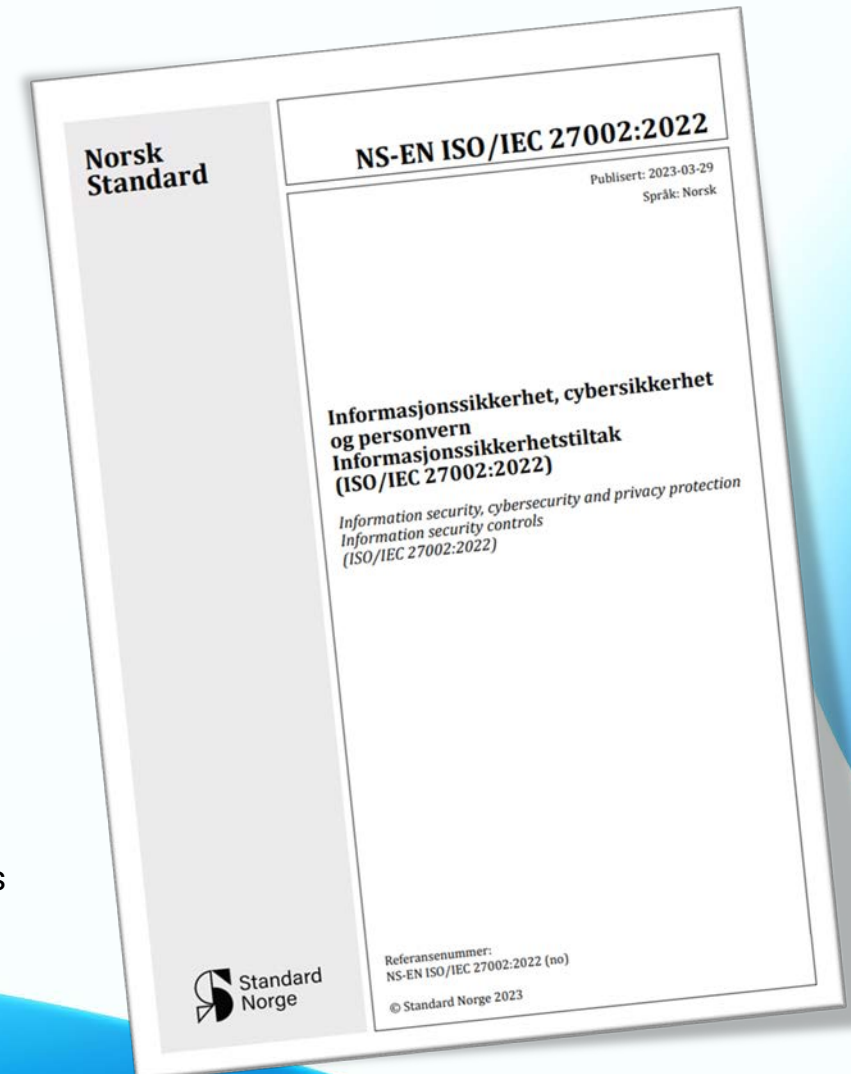
Formål

Å registrere hendelser, generere bevis, sikre integriteten til logininformasjon, forebygge uautorisert tilgang, identifisere informasjonssikkerhetsepisoder som kan føre til en informasjonssikkerhetshendelse, og støtte etterforskninger.

Veiledning

Generelt

Organisasjonen bør fastsette hvilke logger som skal opprettes, hvilke data som skal samles inn og logges, og hvilke loggspesifikke krav som eventuelt skal stilles for å beskytte og håndtere loggdataene.



[Forside](#) / [Presse og nyheder](#) / [Nyhedsarkiv](#) / [2023](#) / [feb](#) /

Modenhedstilsynet i 2022 viser behov for øget fokus på bl.a. sletning og konsekvensanalyse

[Presse og nyheder](#)[Pressefotos](#)[Arkiv over nyheder](#)[Nyhedsbrev](#)

Modenhedstilsynet i 2022 viser behov for øget fokus på bl.a. sletning og konsekvensanalyse

Dato: 23-02-2023

Nyhed

Datatilsynet gennemførte i 2022 et omfattende survey-baseret tilsyn. Tilsynet omfattede 50 kommuner og alle 5 regioner. Modenhedstilsynet giver Datatilsynet et værdifuldt indblik i modenhedsniveauet, og indsigterne herfra er inddraget i planlægningen af Datatilsynets tilsyns- og vejledningsaktiviteter for 2023.



Modenhedstilsynet viser et generelt behov for øget fokus på sletning, rettighedsstyring og foranstaltninger ved fremsendelse af mails med personoplysninger. Derudover indikerer tilsynet, at arbejdet med konsekvensanalyser og test af it-beredskab bør have mere opmærksomhed i kommunerne.

Formålet med modenhedstilsyn

Modenhedstilsyn er baseret på egen-evaluering, og giver Datatilsynet et værdifuldt indblik i modenhedsniveauet hos de dataansvarlige, der indgår i undersøgelsen.

Formålet med egen-evalueringen er at give Datatilsynet blik for bestemte emneområder med behov for øget indsats (tilsyn såvel som vejledning), men også at understøtte en mere forebyggende tilgang hos de dataansvarlige. Gennem den

Tekniske tiltag

Tekniske minimumskrav ^

– Tekniske minimumskrav 2023

Cyberforsvar, der virker

Styring af password

DMARC

Sikring af udstyr i udlandet

Tekniske minimumskrav for statslige myndigheder 2023

De 20 tekniske minimumskrav til sikkerheden i it-løsninger for statslige myndigheder er per 29. juni 2022 blevet opdateret til en 2023-version. Kravene er ufravigelige og skal sikre et fælles højt sikkerhedsniveau i staten.

Som led i den nationale cyber- og informationssikkerhedsstrategi 2022-2024 er de tekniske minimumskrav til it-sikkerhed blevet opdateret. Alle de opdaterede krav skal være implementeret senest den 1. januar 2023.

Oversigt over minimumskravene 2023

Kravene er udtryk for udbredt *best practice* og flere følger af eksisterende vejledninger og anbefalinger på området fra Center for Cybersikkerhed, Digitaliseringsstyrelsen og Datatilsynet.

Klik på de enkelte krav nedenfor for at læse mere om formålet med kravene.

[Klik her for at se alle minimumskrav 2023 i printvenlig version](#)

Ændringslog

De tekniske minimumskrav blev første gang lanceret i 2020. Der er udarbejdet en ændringslog for de opdaterede krav, hvori ændringer per krav fremgår.

[Klik her for at se ændringslog](#)

De tekniske minimumskrav for statslige myndigheder 2023

De 20 tekniske minimumskrav til it-sikkerhed for statslige myndigheder blev i juni 2022 opdateret til en 2023-version. I november 2022 er der foretaget mindre præciseringer til et af kravene samt nogle af kategorierne. Kravene er ufravigelige for statslige myndigheder og skal sikre et fælles højt sikkerhedsniveau i staten. Implementering af kravene skal ske senest d. 1. januar 2023.

Nr.	Kravformulering
Klienter/PC'er: Kr	
1	Der skal implementeres sikkerhed på klienter.
2	Klienter skal benytte Always On VPN fra
3	Klienters harddiske s
4	Der skal implementeres beskyttelse på alle klienter
5	Klienters OS og applikationer skal holdes sikker

Lagring af logs

Et cyberangreb opdages ikke altid, mens det står på. Derfor skal logs gemmes.

Der kan ofte gå uger og måneder fra et angreb sker, til det bliver opdaget. Derfor skal organisationen tage stilling til, hvor længe de enkelte logs skal opbevares. Beslutningen om, hvor længe logs skal opbevares, må tages på baggrund af den enkelte organisations risikovurdering og hensyntagen til regulering på området, der i nogle tilfælde også regulerer, hvor længe logs må opbevares, inden de slettes. Dette bør beskrives i logpolitikken. Logs bør opbevares minimum 13 måneder, medmindre der er lovgivning, der kræver noget andet.

Under lagring skal organisationen sikre sig, at der er etableret de rette sikkerhedsforanstaltninger til at beskytte loggenes integritet, fortrolighed og tilgængelighed. Det betyder for det meste, at de skal beskyttes som organisationens øvrige sensitive informationer, og at der ikke må være adgang for uvedkommende. Det bør sikres, at ingen medarbejdere har mulighed for at manipulere med loggen, uden at det kan opdages.

I forhold til lagring af logs skal organisationen også tage stilling til, hvordan de skal sikkerhedskopieres. Det anbefales, at der sikkerhedskopieres efter samme procedure som for andre sensitive informationer efter organisationens politik på området.

Logning: Kravene til logning angår alle systemer og tjenester på netværksservere.

14	Krav om logning, log på alle systemer og tjenester på netværksservere ²	Formålet med kravet er sikre de bedste forudsætninger for opdagelse af og efterforskning af sikkerhedshændelser. Logningen skal ikke implementeres med formål om at monitorere brugeradfærd.	Kravet er opfyldt, hvis der er implementeret logning i overensstemmelse med CFCS-vejledningen ”Logning af netværkstraf”
----	--	---	---



Er det lov å være litt frustrert over Standard Norge ?



Standard
Norge

Februar 2022

Uke	Mandag	Tirsdag	Onsdag	Torsdag	Fredag	Lørdag	Søndag
5	31	1	2	3	4	5	6
6	7	8	9	10	11	12	13
7	14	 15	16	17	18	19	20
8	21	22	23	24	25	26	27
9	28	1	2	3	4	5	6



ISO/IEC 27002:2022
15.02.2022

Oktober 2022

Uke	Mandag	Tirsdag	Onsdag	Torsdag	Fredag	Lørdag	Søndag
39	26	27	28	29	30	1	2
40	3	4	5	6	7	8	9
41	10	11	12	13	14	15	16
42	17	18	19	20	21	22	23
43	24	 25	26	27	28	29	30
44	31	1	2	3	4	5	6

ISO/IEC 27001:2022
25.10.2022

Mars 2023

Uke	Mandag	Tirsdag	Onsdag	Torsdag	Fredag	Lørdag	Søndag
9	27	28	1	2	3	4	5
10	6	7	8	9	10	11	12
11	13	14	15	16	17	18	19
12	20	21	22	23	24	25	26
13	27	28	 29	30	31	1	2

Norsk
Standard

NS-EN ISO/IEC 27002:2022

Publisert 2023-03-29
Språk: Norsk

Informasjonssikkerhet, cybersikkerhet
og personvern
Informasjonssikkerhetstiltak
(ISO/IEC 27002:2022)
Information security, cybersecurity and privacy protection
Information security controls
(ISO/IEC 27002:2022)



Referansenormer:
NS-EN ISO/IEC 27002:2022 (nvl)
© Standard Norge 2023

ISO/IEC 27002:2022
29.03.2023

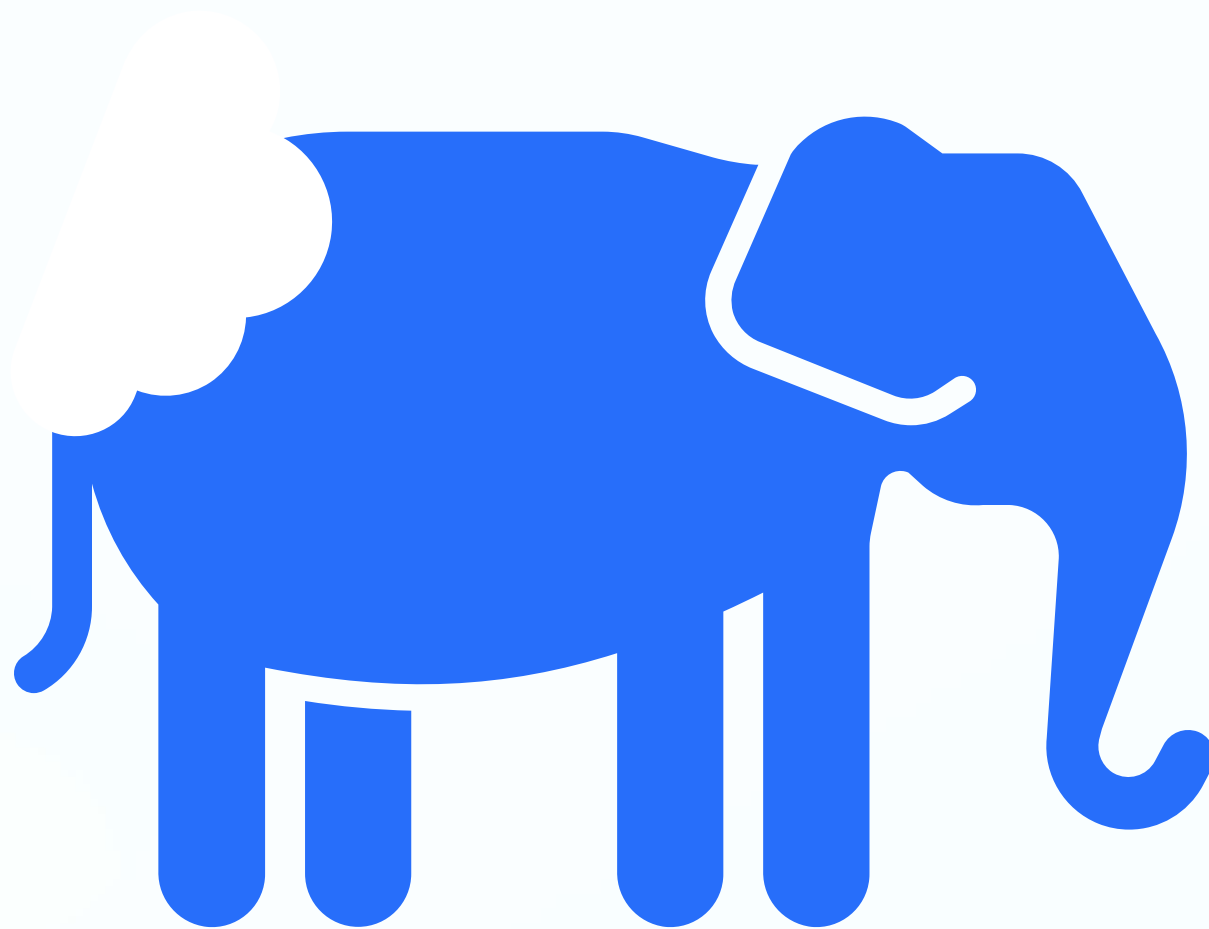
Mai 2023

Uke	Mandag	Tirsdag	Onsdag	Torsdag	Fredag	Lørdag	Søndag
18	1	2	3	4	5	6	7
19	8	9	10	11	12	13	14
20	15	16	17	18	19	20	21
21	22	 23	 24	 25	26	27	28
22	29	30	31	1	2	3	4

Arbeid med  /IEC 27001 involverer hele virksomheten



Hvordan spise en elefant



Takk for oppmerksomheten