Vår saksbehandler
Håkon Jentoft og Emanuela Rokke, tlf. 99498028

Det kongelige Justis- og beredskapsdepartement
Høringsportal

Vår dato 2024-12-09
Vår ref. -----
Deres dato 2024-09-11
Deres ref. 24/3567

Innspill til forslag til forskrift til digitalsikkerhetsloven (digitalsikkerhetsforskriften)

Standard Norge ber departementet vurdere hvordan standarder innen ledelsessystem for IT og risikohåndtering kan hjelpe virksomheter i å nå målsettingene og krav gitt i digitalsikkerhetsforskriften. Vi ber også departementet vurdere hvordan internasjonale standarder kan være et supplerende virkemiddel til forskriften.

Standard Norge viser til invitasjon til å inngi høringsinnspill til forslag om forskrift til digitalsikkerhetsloven (digitalsikkerhetsforskriften) publisert på Justis og beredskapsdepartementets hjemmeside 2024-09-11.

Om Standard Norge og de internasjonale standardiseringsorganisasjonene

Standard Norges mandat som nasjonal standardiseringsorganisasjon er hjemlet i Europaparlaments- og rådsforordning (EU) nr. 1025/2012 om europeisk standardisering, som er iverksatt i norsk rett. Vi viser til tilskuddsbrev for 2024 fra Nærings- og fiskeridepartementet av 2023.12.21 for nærmere beskrivelse av Standard Norges oppgaver knyttet til oppfølging av Innst. 8 S (2023–2024) og Prop. 1 S (2023–2024) for Nærings- og fiskeridepartementet.

Standard Norge er Norges medlem i den internasjonale standardiseringsorganisasjonen ISO og den europeiske standardiseringsorganisasjonen CEN. I tillegg følger Standard Norge EUs arbeid med standardisering tett. EU bruker i økende grad standarder til å konkretisere generelle forordninger. I februar 2022 ga Europakommisjonen ut sin standardiseringsstrategi. Denne suppleres med et årlig arbeidsprogram for standardisering.

Standard Norge har ansvar for standardiseringsoppgaver innenfor de fleste områder. Standarder er et nødvendig og viktig verktøy for å ivareta god sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner. Standarder spesifiserer krav og retningslinjer til prosesser og tjenester innenfor de fleste områder og er et viktig virkemiddel til hjelp med å utvikle systemer for samhandling, forebygging og håndtering av større ulykker og hendelser. Standard Norge ivaretar en nøytral og troverdig prosess og videre vedlikehold av standarder etter utgivelse.

Kommentarer til forslag til forskrift til digitalsikkerhetsloven (digitalsikkerhetsforskriften) fra Standard Norge

I høringsnotatet til forskriftsforslaget står det:

> *Forskriftsforslaget presiserer virkeområdet for tilbydere av samfunnsviktige tjenester, herunder hvilke virksomheter som unntas virkeområdet. Det foreslås at ansvarlig departement i særlige tilfeller kan beslutte at andre virksomheter også underlegges regelverket ved enkeltvedtak. Videre foreslås det å forskriftsfeste at tilbydere av samfunnsviktig tjeneste skal etablere og vedlikeholde et styringssystem for digital sikkerhet. Styringssystemet for digital sikkerhet vil omfatte både digitale, fysiske og personelle sikkerhetstiltak. Det blir foreslått at tilbyderne skal utarbeide risikovurderinger og planer for å håndtere risiko.*

Vår saksbehandler
Håkon Jentoft og Emanuela Rokke, tlf. 99498028

Forskriften vil videre stille krav til at virksomheter må følge spesifikke standarder og retningslinjer for å sikre tilstrekkelig digital sikkerhet. Styringssystem for digital sikkerhet vil kreve at virksomheter må etablere og vedlikeholde et styringssystem som inkluderer digitale, fysiske og personelle sikkerhetstiltak. For risikovurdering og risikohåndtering vil det kreves at virksomheter utfører risikovurderinger og utarbeider planer for å håndtere identifiserte risikoer.

Høringsnotatet nevner bruk av standarder og standardisering flere steder. Standarder utarbeidet av Standard Norge (NS-standarder), CEN (EN-standarder) og ISO (ISO-standarder) angir hvordan et forskriftsfestet krav kan oppnås. Standardene utarbeides av berørte parter. De vil angi beste praksis på et område og er ved utgivelsestidspunktet akseptert av brukerne gjennom den medvirkning og innflytelse de har hatt i arbeidet med standardene.

Det er utarbeidet en rekke standarder som kan hjelpe virksomheter til å etablere ledelsessystemer for informasjonssikkerhet og risikohåndtering. Standardene gjør det mulig å dokumentere/revidere at virksomhetenes ledelsessystemer er etablert og fungerer etter hensikten. Standard Norge har opprettet flere komiteer med oppgave å utarbeide norske standarder samt delta med eksperter i arbeidet med utarbeidelse og revidering av europeiske (CEN) og internasjonale (ISO) standarder. Komiteene er sammensatt med medlemmer berørte virksomheter og myndigheter.

Nedenfor beskrives noe av det arbeidet som pågår:

Ledelsessystem for IT-sikkerhet - **SN/K 171 Informasjonssikkerhet, cybersikkerhet og personvern**

Etablering og implementering av et ledelsessystem for informasjonssikkerhet i en organisasjon påvirkes av organisasjonens behov og mål, sikkerhetskrav, de organisatoriske prosessene som benyttes, samt størrelsen og strukturen på organisasjonen. Alle disse påvirkende faktorene forventes å endre seg over tid. Standardene i ISO/IEC 27000-serien har til hensikt å sikre virksomheters informasjon og å ha et system for dette. Flere av standardene i ISO/IEC 27000-serien er oversatt til norsk.

Et ledelsessystem for informasjonssikkerhet bevarer konfidensialiteten, integriteten og tilgjengeligheten til informasjon ved å benytte en risikostyringsprosess. Dette gir tillit hos interesseparter ved at risikoer er tilstrekkelig håndtert.

ISO/IEC 27001 er verdens mest kjente standard for styringssystemer for informasjonssikkerhet (ISMS). Den definerer krav et ISMS må oppfylle. ISO/IEC 27001-standarden gir selskaper i alle størrelser og fra alle aktivitetssektorer veiledning for å etablere, implementere, vedlikeholde og kontinuerlig forbedre et styringssystem for informasjonssikkerhet.

Samsvar med ISO/IEC 27001 betyr at en organisasjon eller virksomhet har fått på plass et system for å håndtere risiko knyttet til sikkerheten til data som eies eller håndteres av selskapet, og at dette systemet respekterer alle beste praksiser og prinsipper nedfelt i denne internasjonale standarden.

Med økende nettkriminalitet og stadig nye trusler som dukker opp, kan det virke vanskelig eller til og med umulig å håndtere cyberrisiko. ISO/IEC 27001 hjelper organisasjoner med å bli risikobevisste og proaktivt identifisere og adressere svakheter.

ISO/IEC 27001 fremmer en helhetlig tilnærming til informasjonssikkerhet: kontroll av mennesker, retningslinjer og teknologi. Et styringssystem for informasjonssikkerhet implementert i henhold til denne standarden er et verktøy for risikostyring, cyber-resiliens og operasjonell fortreffelighet.

Blant de mest sentrale standardene i serien er:

Vår saksbehandler
Håkon Jentoft og Emanuela Rokke, tlf. 99498028

- NS-EN ISO/IEC 27000 - Holder rede på sammenhengene mellom standardene og begreper som benyttes i serien.

- NS-ISO/IEC 27001 - Stiller krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet. Dette er standarden som det kan sertifiseres i forhold til, og resten av serien er en utdypning og veiledning i forhold til denne standarden.

- NS-EN ISO/IEC 27002 - Gir god praksis i forhold til hva en bør gjøre, hva en bør vurdere og hva en bør ha på plass.

- NS-ISO/IEC 27003 - Skisserer mulige strategier for å iverksette en prosess for å innføre et ledelsessystem for informasjonssikring.

- NS-ISO/IEC 27004 - Hjelper til med hvordan man måler tilstanden før, under og etter innføringen av sikringstiltak.

- NS-ISO/IEC 27005 - Omhandler risikostyring av informasjonssikkerhet.

Risikovurdering og håndtering – Standardiseringskomité SN/K 239 Risiko

ISO 31000-serien er en ledelsesstandard, som stiller krav til hvordan en organisasjon innarbeider systematikk og struktur for å håndtere risiko. Risiko i denne sammenheng er alle mulige typer risiko, og i standarden stilles det krav til hvordan organisasjonen innarbeider forståelse og bevissthet om risiko på alle nivåer. Det anbefales at risikostyring er en del av organisasjonens struktur, prosesser, mål, strategi og aktiviteter. Følgende standarder er utarbeidet i serien:

- ISO 31000:2018 Risikostyring –gir veiledning om hvordan organisasjoner kan integrere risikobasert beslutningstaking i styring, planlegging, ledelse, rapportering, policy, verdier og kultur. Det er et åpent, prinsippbasert system, som betyr at det er mulig for organisasjonen å anvende prinsippene i standarden til egen kontekst. Dette dokumentet kan brukes på enhver aktivitet i en organisasjon, inkludert beslutningstaking på alle nivåer.

- IEC 31010:2019 Metoder for risikovurdering - er en generell standard som kan brukes av alle som skal utføre risikovurderinger. Ulike situasjoner og prosesser krever ulike metoder når risiko skal vurderes, og en rekke risikovurderingsmetoder og deres fordeler og ulemper er beskrevet i standarden.

- ISO/TS 31050:2023 Risk management - Guidelines for managing an emerging risk to enhance resilience – utfyller ISO 31000 og gir veiledning om håndtering av nye risikoer som en organisasjon kan møte. Dette dokumentet gjelder for enhver organisasjon, på ethvert stadium og for enhver aktivitet i organisasjonen. Applikasjonen kan tilpasses for å passe forskjellige organisasjoner eller konteksten til forskjellige organisasjoner.

Det er også utarbeidet norske standarder for risikovurdering:

- NS 5814 Krav til risikovurderinger

- NS 5840 Beredskapsvurderinger

I den nasjonale standarden NS 5814 Krav til Risikovurderinger angis det konkrete krav til gjennomføringen av risikovurderingsprosessen med en trinnvis beskrivelse av aktiviteter og vurderinger. Standarden peker på at både sannsynlighet for en begivenhet og konsekvensen av en inntruffet begivenhet inngår i risikovurderingen.

Vår saksbehandler
Håkon Jentoft og Emanuela Rokke, tlf. 99498028

NS 5840 Krav til beredskapsvurderinger inneholder krav til metodikk for å konkretisere, planlegge og vurdere effekten av konkrete tiltak som respons på utvalgte scenarier. Dette konkretiserer utformingen av de konkrete tiltakene man bør planlegge for. Standarden angir hvordan man skal planlegge og etablere beredskapsløsninger som svar på ulike konsekvenser.

Standard Norge ber departementet vurdere hvordan standarder innen ledelsessystem for IT og risikohåndtering kan hjelpe virksomheter i å nå målsettingene og krav gitt i den nye digitalsikkerhetsforskriften. Standard Norge vil påpeke at IT risiko er en global utfordring. Europeiske og internasjonale standarder kan bidra til at virksomheter på tvers av landegrenser innfører sammenlignbare ledelsessystemer og gjennom dette lettere kan motvirke risiko fra globale aktører. Vi ber derfor departementet vurdere hvordan internasjonale standarder kan være et supplerende virkemiddel til forskriften.

Standard Norge bidrar gjerne med mer utfyllende informasjon i eget møte med departementet.

Vennlig hilsen,

Åse Lunde
Direktør Energi, bærekraft og teknologi