Mattilsynet

DIGITAL-SIKKERHETSFORSKRIFTEN FOR DRIKKEVANN

Om veilederen (første versjon 16.06.26)

Veilederen forklarer kravene i digitalsikkerhetsforskriften (dsf) for norske vannverk. Dsf gjelder fra oktober 2025. Vannforsyningssystem som produserer minst 2000 m^3 per døgn, jf. drikkevannsforskriften § 3 bokstav k og bokstav f, er underlagt kravene i dsf.

For mindre vannforsyningssystem, der farekartleggingen viser risiko for å bli utsatt for cybertrusler eller -hendelser, gjelder kravene i drikkevannsforskriften (dvf). For disse kan dsf og denne veilederen benyttes som hjelpemiddel i arbeidet med digital sikkerhet, men kravene i dsf gjelder ikke direkte.

Veilederen presenterer kravene i dsf, forklarer viktige ord i lovtekst og gir veiledning på hvordan kravene kan etterleves. Veilederen gir også lenker til nyttige ressurser som standarder, sjekklister, temaveiledere og fagrapporter. Veilederen er utarbeidet av Mattilsynet.

Spørsmål og kommentarer til veiledningen kan rettes til Mattilsynet på e-post
digitalsikkerhet@mattilsynet.no

Innhold

Veilederens struktur og oppbygging

Veilederen til digitalsikkerhetsforskriften og -loven er rettet mot vannverk og deres ansvar for å sikre digitale systemer. Den gir råd om hvordan virksomheten kan etterleve regelverkets krav. Veilederen følger forskriftens struktur og inneholder korte beskrivelser av krav, gjengivelse av bestemmelser, relevante ordforklaringer og tolkning av hva som kreves i praksis. I forbindelse med de enkelte bestemmelsene vises det avslutningsvis til nyttige kilder samt krysskoblinger til tilknyttede og relevante paragrafer og regelverk. Ved å krysskoble til andre paragrafer blir det lettere å se kravene i sammenheng.

Forholdet mellom digitalsikkerhetsregelverket og annet sektorregelverk

Etter digitalsikkerhetsloven § 5 gjelder lovens krav om sikkerhet og varsling så langt det ikke er fastsatt tilsvarende eller strengere krav i annet regelverk. Digitalsikkerhetsregelverket fungerer dermed som et overordnet rammeverk med minimumskrav til sikring av nettverks og informasjons-systemer på tvers av sektorer, samtidig som sektorer kan ha egne, tilpassede krav. Drikkevannsforskriften § 6 krever at vannverkseier identifiserer og gjennomfører tiltak for å forebygge, fjerne eller redusere farer til et akseptabelt nivå. Dette inkluderer farer knyttet til nettverks- og informasjons-systemer. Kravene i digitalsikkerhetsforskriften og drikkevannsforskriften vil derfor delvis overlappe og utfylle hverandre. Av hensyn til forutberegnelighet og klarhet for virksomheter som omfattes av både dsf og dvf, vil vedtak ved manglende etterlevelse av krav knyttet til digital sikkerhet gis med hjemmel i dsf.

1. Innmeldingsplikt

1.1 Ingress

Virksomheter som omfattes av digital sikkerhetsloven plikter å registrere seg for NSM og Mattilsynet.

1.2 Krav

---

§ 5.Innmelding av tilbydere av samfunnsviktig tjeneste

Tilbydere av en samfunnsviktig tjeneste skal snarest melde inn til Nasjonal sikkerhetsmyndighet og tilsynsmyndigheten opplysninger om

a. virksomhetens navn, organisasjonsnummer og kontaktinformasjon

b. tjenesten

c. samfunnssektor

d. i hvilke andre land tjenesten tilbys

e. berørt geografisk område

1.3 Ordforklaring

Ord	**Ordforklaring**
Tjeneste	Her: Distribusjon og levering av helsemessig trygt drikkevann
Samfunnssektor	Her: Vannforsyning

1.3 Hvordan oppfylle kravet?

- Virksomheten skal fylle ut ett skjema for innmelding av *virksomheten* og ett skjema for innmelding av *tjeneste*.
- Innmeldingen skal angi tjeneste, samfunnssektor, i hvilke andre land tjenesten tilbys og berørt geografisk område.
- Under kontaktinformasjon bør virksomheten oppgi hvem som er virksomhetens kontaktperson for innmeldingen, telefonnummer, telefonnummer til en vakttelefon ved hendelser, e-postadresse, fysisk adresse og postadresse.
- Innmeldingsskjemaene skal sendes på e-post, merket «Innmelding digital sikkerhetsloven», til postmottak@nsm.no og postmottak@mattilsynet.no.
- Innmelding skal foretas uten ugrunnet opphold.

1.4 Ressurser

- Skjema for innmelding av virksomhet
- Skjema for innmelding av samfunnsviktige tjenester

2. Styringssystem for informasjonssikkerhet

2.1 Ingress

Virksomheten skal ha et styringssystem for informasjonssikkerhet som opprettholder et forsvarlig sikkerhetsnivå. Systemet skal bygge på anerkjente standarder.

2.2 Krav

---

§ 6 Styringssystem for sikkerhet

En tilbyder av en samfunnsviktig tjeneste skal etablere og vedlikeholde et styringssystem for sikkerhet som omfatter digital sikkerhet. Styringssystemet skal dokumenteres og inngå som del av den overordnede virksomhetsstyringen. Roller og ansvar for digital sikkerhet skal defineres, utpekes og dokumenteres.

Sikkerhetsstyringssystemet skal baseres på anerkjente standarder og bidra til å

a. forebygge hendelser

b. avdekke hendelser

c. håndtere hendelser

d. korrigere og gjenopprette sikkerheten i nettverk og informasjonssystemer ved hendelser

e. kontinuerlig styre og følge opp at formålene i bokstavene a til d oppnås.

Alle aktiviteter som er nødvendige for å etablere og opprettholde et forsvarlig sikkerhetsnivå skal inngå i sikkerhetsstyringssystemet. Aktivitetene skal dokumenteres og gjøres kjent for personell med tjenstlig behov.

Virksomhetens leder har ansvaret for at virksomheten har et forsvarlig sikkerhetsnivå innenfor virkeområdet til digitalsikkerhetsloven. Sikkerhetsstyringssystemet skal godkjennes av virksomhetens leder og gjennomgås minst årlig med sikte på å forbedre virksomhetens sikkerhetsarbeid.

2.3 Ordforklaring

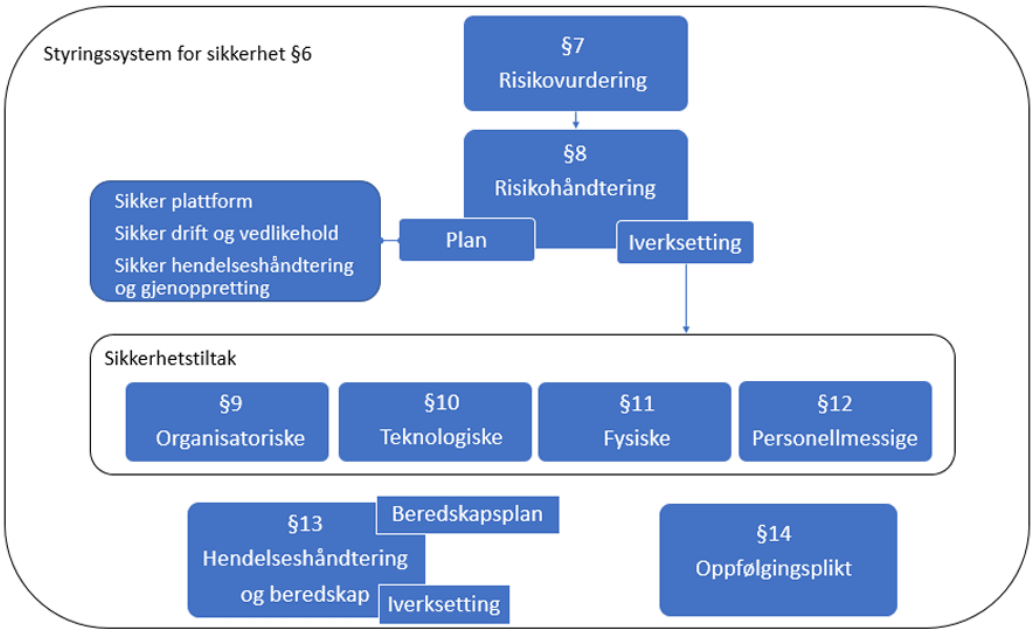
Ord	Forklaring
Styrings-system	Et system som gir uttrykk for virksomhetens mål, prosesser, roller, tiltak og kontroller som virksomheten bruker for å planlegge, gjennomføre, følge opp og ivareta et forsvarlig sikkerhetsnivå.
Forsvarlig sikkerhetsnivå	En rettslig standard som endrer seg over tid basert på utviklingen i marked, teknologi og samfunn. Hva som anses som forsvarlig sikkerhetsnivå kan variere mellom ulike vannverk, basert på deres risikovurderinger og det til enhver tid gjeldende trusselbilde.
Nettverks- og informasjons-systemer	Digitalsikkerhetsloven § 4 definerer nettverks- og informasjonssystemer som: a. elektronisk kommunikasjonsnett som nevnt i ekomloven § 1-5 nr. 2 b. en enhet eller en gruppe av sammenkoblede eller beslektede enheter som behandler digitale data automatisk ved hjelp av et program c. digitale data som lagres, behandles, innhentes eller overføres ved hjelp av elementer som nevnt i bokstav a eller b for at dataene skal kunne driftes, vernes, beskyttes eller vedlikeholdes. Begrepet omfatter både informasjonsteknologi (IT) og industrielle kontrollsystemer (operasjonell teknologi (OT)), også kalt driftskontrollsystemer. OT inkluderer prosess- og kontrollsystemer som overvåker og styrer prosesser i vannbehandlings- og avløpsrenseanlegg.
Digitale systemer	Her: Synonymt med nettverks- og informasjonssystemer
Tilbyder	Her: Vannverk
Sikkerhet	Sikkerhet i digitale systemer er evnen digitale systemer har til å tåle, på et gitt tillitsnivå, enhver handling som går ut over tilgjengeligheten, autentisiteten, integriteten eller konfidensialiteten til lagrede, overførte og behandlede data, eller tilknyttede tjenester som tilbys eller er tilgjengelige via slike digitale systemer.

2.4 Hvordan oppfylle kravet?

For å oppfylle kravet skal virksomheten, som minimum:

- Etablere og vedlikeholde et dokumentert styringssystem for digital sikkerhet over tid (sikkerhetsstyringssystem). Sikkerhetsstyringssystemet kan inngå som en del av internkontrollen, så lenge digital sikkerhet adresseres særskilt i denne.
- Sørge for at sikkerhetsstyringssystemet bygger på sikkerhetsstandarder, for eksempel ISO/IEC 27001 *Ledelsessystemer for informasjonssikkerhet*, eller NSMs grunnprinsipper for sikkerhetsstyring. Mattilsynet anbefaler NSMs grunnprinsipper for sikkerhetsstyring.
- Ha definert sikkerhetsroller og tydeliggjort sikkerhetsansvar for medarbeidere og ledere. Det skal som minimum utpekes en ansvarlig for virksomhetens digitale sikkerhet. Rollene og ansvaret skal formaliseres skriftlig, og personell med tjenstlig behov skal ha kjennskap til aktiviteter i virksomhetens sikkerhetsstyringssystem. Eksempel på aktivitet kan være opplæring, beredskapsøvelser og leverandøroppfølgning.
- Sørge for at sikkerhetsstyringssystemet er samkjørt med virksomhetens øvrige styringssystem, og at det er faktisk gjennomførbart.
- Sørge for at sikkerhetsstyringssystemet godkjennes av virksomhetens leder.
- Ved behov, men minst årlig, kontrollere sikkerhetsstyringssystemet og sørge for at svakheter blir utbedret.

Sikkerhetsstyringssystemet skal utgjøre summen av alle kravene digitalsikkerhetsforskriften oppstiller. Den samlede strukturen av mål, prosesser, roller, tiltak og kontroller skal derfor sikre at virksomheten oppnår et forsvarlig sikkerhetsnivå.



Figur 1 Sikkerhetsstyringssystem og sammenheng med kravene i digital sikkerhetsloven (Kilde: NSM)

Eksempel på dokumenter som kan inngå i sikkerhetsstyringssystemet

- Virksomhetens sikkerhetspolitikk, som er et ledelsesdokument, hvor virksomhetens overordnede sikkerhetsmål beskrives.
- Retningslinjer for sikring av digitale systemer, eks IT og driftskontrollsystemer (OT)
- Retningslinjer for å gi digital og fysisk tilgang til leverandører som skal utføre service på kontrollanlegg
- Retningslinjer for ansattes bruk av virksomhetens IT-system
- Retningslinjer for ansattes sikkerhet på reise
- Retningslinjer for trygg bruk av kunstig intelligens
- Retningslinjer for sikker utvikling av programvare
- Retningslinjer for fysisk sikring av digitale systemer, for eksempel låste datarom
- Retningslinjer for leverandørers fjerntilgang til OT-systemer
- Prosedyre for risikoanalyse og risikostyring
- Beredskapsplan for hendelseshåndtering i IT- og OT-systemer

OBS! Styringssystemet bør ta inn i dokumentasjon fra andre aktuelle lov- og forskriftskrav. Her er det viktig å være kjent med at **digitalsikkerhetsloven § 5 regulerer *forholdet til andre lover som stiller krav om sikkerhet og varsling*** Kravene til sikkerhet og varsling i digitalsikkerhetsforskriften §§ 7, 8, 10 og 11 gjelder så langt det ikke er fastsatt tilsvarende eller strengere krav i eller i medhold av annen lov.

Drikkevannsforskriften setter krav som bidrar til å sikre levering av helsemessig trygt drikkevann. Digitalsikkerhetsforskriften understøtter drikkevannsforskriftens formål ved å bidra til å sikre IT og OT-systemer hos vannverk.

2.5 Ressurser

NSMs Grunnprinsipper for sikkerhetsstyring

Utstyrsoversikt, ansvar og rutiner for operasjonell teknologi - Norsk helsenett

Veileder fra NSM i digitalsikkerhetsloven og -forskriften.pdf, se side 27

Veileder til drikkevannsforskriften | Mattilsynet, se veiledning til § 10

Ledelsessystemer for informasjonssikkerhet – ISO/IEC 27001

NIS2 Technical Implementation Guidance | ENISA

Cybersecurity Framework | NIST

2.6 Kobling til annet regelverk

Drikkevannsforskriften § 7 Internkontroll

Drikkevannsforskriften § 9 Leveringssikkerhet

Drikkevannsforskriften § 10, Forebyggende sikring (fysisk og digital)

Drikkevannsforskriften § 11 Beredskap (planer og øvelser)

Digitalsikkerhetsloven

Lov om nasjonal sikkerhet (sikkerhetsloven) - Lovdata

3. Risikovurdering

3.1 Ingress

Virksomhetene skal gjennomføre risikovurdering. Risikovurderingen danner grunnlaget for å bestemme forsvarlig sikkerhetsnivå utover de minimumskrav til tiltak som digitalsikkerhetsforskriften oppstiller.

3.2 Krav

---

§ 7 Risikovurdering

Risikovurderingene skal være av et slikt omfang at tilbyderen kan identifisere organisatoriske, teknologiske, fysiske og personellmessige sikkerhetstiltak som ivaretar formålene i § 8 andre ledd. Ved endringer i virksomheten som kan påvirke sikkerheten, skal tilbyderen vurdere hvilken risiko endringene medfører.

Risikovurderingene skal minst beskrive

a. virksomhetens nettverk og informasjonssystemer og hvilken betydning disse har for leveransen av den samfunnsviktige tjenesten

b. hvilke hendelser virksomhetens nettverk og informasjonssystemer kan bli utsatt for

c. hvilke sårbarheter som er knyttet til virksomhetens nettverk og informasjonssystemer

d. konsekvensen av hendelser

e. i hvilken grad virksomheten er avhengig av andre virksomheter for å fungere som den skal.

3.3 Ordforklaring

Ord	Ordforklaring
Risiko	Ofte omtalt som usikkerhet eller uvisshet multiplisert med konsekvens
Risikovurdering	Systematisk metode for å identifisere og evaluere farer og trusler.
Hendelser	Enhver hendelse med negativ virkning på sikkerheten i nettverks- og informasjonssystemer, jf. digitalsikkerhetsloven § 4 Dette omfatter alle mulige hendelser som kan skade eller redusere funksjonaliteten til det digitale systemet. Det dekker naturgitte hendelser, som lyn, flom, brann mv., og menneskeskapte hendelser som driftsfeil, tap av kompetanse, datainnbrudd, sabotasje mv.
Konsekvens	Skade, ødeleggelse, begrensning eller reduksjon av det digitale systemets funksjon, og derigjennom vannverkets evne til å levere helsemessigtrygt drikkevann.

3.4 Hvordan oppfylle kravet?

For å oppfylle kravet skal virksomheten, som minimum:

- Gjennomføre risikovurdering av virksomhetens digitale systemer. Det finnes ulike metoder for gjennomføring av risikovurderinger, og hvilken metode som benyttes er ikke avgjørende. Virksomheten kan foreta en overordnet risikovurdering som dekker hele IT- og OT-miljøet, uten å vurdere alle systemer i detalj. Basert på denne risikovurderingen, kan de delene av systemet med en identifisert høyere risiko vurderes grundigere.
- Identifisere hendelser som kan ramme det digitale systemet. Bruk gjerne idemyldring til å identifisere mulige og reelle hendelser.
- Identifisere sårbarheter. I vurderingen av sårbarhet, skal avhengigheten til leverandører av digitale tjenester vurderes. Andre sårbarheter kan være ikke sikkerhetsoppdaterte programvarer, svake og utdaterte passord, samt uklare roller og ansvar.
- Vurdere hvilke konsekvenser materialisering av identifiserte hendelser og sårbarheter vil ha for systemets funksjonalitet. Vurder deretter, hvilke konsekvenser et eventuelt funksjonalitetstap vil ha for befolkningens tilgang til trygt drikkevann.

- Re-evaluere risikovurderingen ved behov, men minst årlig. Behovet kan skyldes endringer i virksomheten eller i trusselbildet.

Mattilsynet anbefaler å velge en anerkjent standard eller veiledning som utgangspunkt for risikovurderingen. Dette for å sikre en systematisk og helhetlig risikovurdering.

Risikovurdering

NSM har utarbeidet et enkelt verktøy for risikovurdering av (ugraderte) IKT-systemer. Dette verktøyet kan benyttes enten det gjelder informasjonssystem (IKT), industrielle kontrollsystemer (OT) eller andre støttesystemer som inngår i porteføljen for IKT-systemer. Det er også utarbeidet et eget regneark som kan brukes som mal til å gjennomføre risikovurderinger.

NSM Veileder for risikovurdering av IKT-systemer (m. lenke til regnearkverktøy)

3.5 Ressurser

NS 5814 – En overordnet og generell standard for risikovurderinger som omfatter både tilsiktede og utilsiktede hendelser.

NS 5832– En mer spesialisert standard for risikovurdering av tilsiktede handlinger, som for eksempel sabotasje og cyberangrep.

NS-ISO/IEC 27005 – En spesialisert standard for digitale/informasjonsrelaterte risikoer.

NS-IEC 31010 – En standard som gir oversikt over metoder og teknikker for risikovurderinger.

NIST SP 800-30 – Veiledning for gjennomføring av risikovurderinger innen informasjonssikkerhet, med særlig vekt på analyse av trusler, sårbarheter og konsekvenser i IT-systemer.

Veiledning for risikovurdering av IT og OT - utarbeidet av Norges vassdrags og energidirektorat

3.6 Kobling til annet regelverk

Drikkevannsforskriften § 6 Farekartlegging og farehåndtering

Forskrift om krav til beredskapsplanlegging og beredskapsarbeid mv. etter lov om helsemessig og sosial beredskap - Lovdata, se § 3 ROS

3.7 Krysskobling

§ 6 Styringssystem for sikkerhet

§ 8 Risikohåndtering, annet ledd

4. Risikohåndtering

4.1 Ingress

Virksomheten skal ha en plan for å håndtere risikoen(e) som er identifisert i risikovurderingen.

4.2 Krav

---

§ 8.Risikohåndtering

Basert på risikovurderingene i § 7 skal en tilbyder av en samfunnsviktig tjeneste ha en plan for å håndtere risiko. Som en del av risikohåndteringen skal tilbyderen iverksette organisatoriske, teknologiske, fysiske og personellmessige sikkerhetstiltak for å redusere risiko og opprettholde et forsvarlig sikkerhetsnivå.

Sikkerhetstiltakene skal som et minimum ha som formål å bidra til sikker plattform, sikker drift og vedlikehold, samt sikker hendelseshåndtering og gjenoppretting.

4.3 Ordforklaring

Ord	**Ordforklaring**
Risikohåndtering	Handlinger og tiltak som bidrar til å fjerne eller redusere uønskede konsekvenser for virksomhetens digitale systemer og tjenesteleveranse.
Sikker	Så langt som praktisk mulig et fravær av at uønskede hendelser oppstår.
Plattform	Plattform kan forstås som det teknologiske fundamentet som muliggjør tjenesten og inkluderer både nettverk, servere, datasenter-tjenester og informasjonssystemer ellers.

4.4 Hvordan oppfylle kravet?

For å oppfylle kravet skal virksomheten, som minimum:

- Utarbeide, dokumentere og gjennomføre tiltaksplaner som tydelig beskriver hvilke organisatoriske, teknologiske, fysiske og personellmessige tiltak som skal iverksettes innenfor de ulike kategoriene. Tiltaksplanene skal redusere

sannsynligheten for, og konsekvensen av, at identifiserte sårbarheter og mulige hendelser aktualiseres. Det skal gå frem av tiltaksplanen hvem som har ansvaret for gjennomføringen av tiltakene.

- Avklare restrisiko og beslutte hvilken restrisiko virksomheten kan akseptere.
- Vurdere og oppdatere tiltaksplaner ved behov, men minst årlig. Behovet kan skyldes endringer i virksomheten eller i trusselbildet.

Vedlikeholdsplan

Planlagte tiltak og andre aktiviteter knyttet til risikohåndtering kan innarbeides i virksomhetens vedlikeholdsplan. I vedlikeholdsplanen kan det angis hvilke digitale systemer, eller deler av systemer, som skal oppdateres eller repareres, samt frister for dette. Planer kan legges i digitale systemer som kobler arbeidsordrer til kalenderplanlegging, utstyrshistorikk, sjekklister, godkjenninger mv.

4.5 Ressurser

ISO 9001 - Ledelsessystemer for kvalitet

ISO/TS 31050:2023 - Guidelines for managing an emerging risk to enhance resilience

4.6 Kobling til annet regelverk

Drikkevannsforskriften § 6 Farekartlegging og farehåndtering

Drikkevannsforskriften § 10

4.7 Krysskobling

§ 6 Styringssystem for sikkerhet

§ 7 Risikovurdering

§ 9 Organisatoriske sikkerhetstiltak

§ 10 teknologiske sikkerhetstiltak

§ 11 Fysiske sikkerhetstiltak

5. Organisatoriske sikkerhetstiltak

5.1 Ingress

Virksomheten skal ha organisatoriske sikkerhetstiltak (styringsdokumenter og tiltaksplaner) som er tilpasset virksomheten og risikoen som virksomheten er utsatt for.

5.2 Krav

---

§ 9.Organisatoriske sikkerhetstiltak

En tilbyder av en samfunnsviktig tjeneste skal utarbeide skriftlige instrukser, rutiner og prosedyrer for digital sikkerhet. Styringsdokumentene skal tilpasses virksomhetens størrelse, kompleksitet og risikobilde.

En tilbyder av en samfunnsviktig tjeneste skal ha oppdaterte tiltaksplaner som kan iverksettes dersom risikoen endrer seg eller det oppstår en hendelse, jf. § 13.

Styringsdokumentene og tiltaksplanene etter første og andre ledd skal gjøres kjent for personell som utfører oppgaver for eller på vegne av virksomheten og som kan få tilgang til virksomhetens nettverk og informasjonssystemer.

5.3 Ordforklaring

Ord	**Ordforklaring**
Styringsdokumenter	Interne dokumenter som gir overordnede føringer og krav for virksomhetens styring og aktivitet. De består av instrukser, rutiner og prosedyrer for digitale systemer og utgjør en del av virksomhetens samlede styringssystem.
Instruks	Overordnet krav og prosedyrer til hvordan man skal handle og opptre.
Rutine	Vane eller fast praksis, ofte innarbeidet på bakgrunn av en prosedyre.
Prosedyre	Detaljert og trinnvis beskrivelse av hvordan et arbeid skal utføres.

5.4 Hvordan oppfylle kravet?

For å oppfylle kravet skal virksomheten, som minimum:

- Utarbeide gode styringsdokumenter, herunder instrukser, rutiner og prosedyrer for digital sikkerhet.
- Sørge for at personell og mottakere av styringsdokumentene er kjent med disse. Graden av kjennskap til dokumentets innhold bør ta utgangspunkt i rollen mottakeren har i virksomheten. For eksempel vil en koordinator ha behov for å være orientert om dokumentet uten å ha inngående kjennskap til innholdet, mens en leder vil ha ansvar for dokumentets innhold og må derfor ha god kjennskap til dets innhold.
- Utarbeide planer med organisatoriske tiltak for å styrke den digitale sikkerheten. Dette kan være, men er ikke begrenset til, vedlikeholdsplaner, forsterkningsplaner på sikkerhet og beredskapsplaner.

Styrende dokumenter

En virksomhets-sikkerhetspolicy beskriver virksomhetens og ledelsens mål og visjon for sikkerhetsarbeidet i virksomheten. Med utgangspunkt i denne policyen kan det lages mer detaljerte instrukser og prosedyrer for ansattes bruk av IT, for sikring og drift av driftskontrollsystemer (OT) og IT, for gjennomføring av risikovurderinger og utvikling av programvare mv.

5.5 Ressurser

Veileder for kartlegging av digital sikkerhetskultur | Digdir

5.6 Kobling til annet regelverk

Digitalsikkerhetsloven § 4 Definisjoner

5.7 Krysskobling

§ 6 Styringssystem for sikkerhet

6. Teknologiske tiltak

6.1 Ingress

Virksomheten skal innføre teknologiske sikkerhetstiltak. Tiltakene skal baseres på risikovurderingen.

6.2 Krav

---

§ 10.Teknologiske sikkerhetstiltak

Basert på risikovurderingen etter §7 skal en tilbyder av en samfunnsviktig tjeneste iverksette teknologiske sikkerhetstiltak som er tilpasset omfang, kompleksitet, driftsmiljø, brukermiljø, funksjon og risiko ved virksomhetens nettverk og informasjonssystemer.

Teknologiske sikkerhetstiltak skal minst omfatte:

a. sterk autentisering for adgang til nettverk og informasjonssystemer

b. styring av og kontroll med tilganger til virksomhetens nettverk og informasjonssystemer

c. tiltak for segmentering av nettverk og tjenester basert på minste privilegiums prinsipp

d. tiltak som skal sikre at nettverk og informasjonssystemer kan håndtere forskjellige typer avbrudd og gjenopprettes innen rimelig tid uten vesentlig reduksjon av tjenestens kvalitet

e. tiltak som skal sikre at nettverk og informasjonssystemer har tilstrekkelig kapasitet til å tåle overbelastning og utstyrssvikt

f. tiltak som skal sikre at nettverk og informasjonssystemer videreutvikles kontinuerlig, herunder at oppdateringer kvalitetssikres, installeres og testes fortløpende

g. sikkerhetsovervåkning av nettverk og informasjonssystemer for å avdekke hendelser.

Dersom et eller flere av tiltakene i andre ledd ikke kan gjennomføres, skal dette godkjennes av virksomhetens leder. Begrunnelsen for unntaket skal dokumenteres i styringssystemet for sikkerhet. Tilsynsmyndigheten skal orienteres om unntaket.

6.3 Ordforklaring

Ord	Ordforklaring
Autentisering	Autentisering er innen IT både prosessen med å bekrefte en påstått identitet, og prosessen med å bekrefte om informasjon er ekte og uendret.
Sterk autentisering	Sterk *autentisering* er som hovedregel en form for autentisering der man bruker flere faktorer (flerfaktorautentisering), for eksempel noe man er (fingeravtrykk), noe man har (bankkort) og/eller noe man vet (passord). Styrken ligger i at flere faktorer benyttes, slik at man er mindre sårbar for innbrudd i IT-systemet dersom én faktor (eks. passord) er lekket.
Adgang	Synonymt her med tilgang.
Segmentering	Inndeling i sikkerhetssoner med tilgangsstyring
Minste privilegiums prinsipp	Enhver bruker har kun tilgang til det som trengs av systemressurser og data/informasjon for brukerens legitime behov.
Nettverk	Elektronisk kommunikasjonsnettverk, datanettverk.
Virksomhetens leder	Administrerende direktør, toppleder.

6.4 Hvordan oppfyllet kravet?

For å oppfylle kravet skal virksomheten, som minimum ha:

a.	sterk autentisering for adgang til nettverk og informasjonssystemer	Virksomheten skal etablere kontrollmekanismer som sikrer at det kun er legitime brukere med en bekreftet identitet som har adgang til virksomhetens digitale systemer. Der det er støttet gir bruk av passnøkkel en sterk autentisering. Dersom passnøkkel ikke er tilgjengelig, er flerfaktorautentisering en aktuell løsning.
b.	styring av og kontroll med tilganger til virksomhetens nettverks- og informasjonssystemer	Virksomheten skal ha tekniske mekanismer og rutiner for å kontrollere brukeres tilganger til digitale systemer. Dette kan for eksempel være etablerte rutiner og teknisk tilgangsstyring når en ansatt får ny stilling eller slutter, eller en nyansatt medarbeider starter i virksomheten. Tilgangsstyring er relevant også for leverandører og applikasjoner. Se NSMs Grunnprinsipper, 2 *Beskytte og opprettholde*.

c.	tiltak for segmentering av nettverk og tjenester basert på minste privilegiums prinsipp	Virksomhetens nettverk skal deles inn i mindre soner. Tilgang til hver sone skal baseres etter prinsippet om minste privilegium, slik at kun autentiserte og autoriserte brukere med et legitimt behov gis tilgang. Se NSMs Grunnprinsipper 2.2 *Etabler en sikker IKT-arkitektur*.
d.	tiltak som skal sikre at nettverk og informasjonssystemer kan håndtere forskjellige typer avbrudd og gjenopprettes innen rimelig tid uten vesentlig reduksjon av tjenestens kvalitet	Virksomheten skal ha evne til å oppdage svikt i digitale systemer og til å håndtere svikten. Se NSMs Grunnprinsipper 3.1 *Oppdag og fjern kjente sårbarheter og trusler* og 4.1 *Forbered virksomheten på håndtering av hendelser*.
e.	tiltak som skal sikre at nettverk og informasjonssystemer har tilstrekkelig kapasitet til å tåle overbelastning og utstyrssvikt	Virksomheten skal være beredt til å håndtere overbelastning av nettverk og utstyrssvikt. Se NSMs Grunnprinsipper for IKT-sikkerhet 4.1 *Forbered virksomheten på håndtering av hendelser*.
f.	Tiltak som skal sikre at nettverk og informasjonssystemer videreutvikles kontinuerlig, herunder at oppdateringer kvalitetssikres, installeres og testes fortløpende	Virksomheten skal installere sikkerhetsoppdateringer så fort som mulig etter at en oppdatering er kunngjort, samt etablere, verifisere og vedlikeholde sikkerhetskonfigurasjonen på alle enheter. Planer for dette bør inngå i sikkerhetsstyringssystemet. Alle endringer, inkludert sikkerhetsoppdateringer, videreutvikling av digitale systemer og innføring av ny teknologi, må testes før de tas i bruk. Ved endringsbehov må virksomheten gjennomføre risikovurderinger og innføre tiltak som reduserer risikoen. NSMs støtteprodukter for NSMs Grunnprinsipper for IKT-sikkerhet gir dere et verktøy.
g.	sikkerhetsovervåkning av nettverk og informasjonssystemer for å avdekke hendelser.	Virksomheten skal ha oversikt over sikkerheten i digitale systemer og være i stand til å avdekke hendelser. Se NSMs Grunnprinsipper for IKT-sikkerhet 3.2 *Etabler sikkerhetsovervåkning*.

Dersom et eller flere av tiltakene i bokstav a til g ikke kan gjennomføres, skal dette godkjennes av virksomhetens leder. Begrunnelse for unntaket skal dokumenteres i sikkerhetsstyringssystemet og kompenserende tiltak skal vurderes.

Mattilsynet skal orienteres om unntaket per e-post merket «digitalsikkerhetsforskriften».

Generelt anbefaler Mattilsynet at virksomheten:

- Har en praksis som er i samsvar med NSMs grunnprinsipper for IKT-sikkerhet som dekker tiltak i kategori 1 og 2. NSMs Grunnprinsipper for IKT-sikkerhet innføres trinnvis, slik at tiltak i kategori 1 innføres først, deretter tiltak i kategori 2. Den gradvise opptrappingen er ment å sikre at grunnsikring er på plass før tilleggssikringen innføres. Tiltak i Kategori 2 forutsetter derfor at tiltak i kategori 1 allerede er på plass. For store virksomheter, eller basert på risikovurdering, må virksomheten inkludere relevante tiltak i kategori 3.
- Ser til NSMs Grunnprinsipper for sikkerhetsstyring eller aktuelle standarder for sikkerhetsstyring.
- Benytter standarder. Ulike standarder har ofte mye felles, og man kan velge den standarden som passer virksomheten best, og supplere med tiltak fra andre standarder og rammeverk dersom relevant.
- Knytter seg til en CERT-tjeneste.

Sikring av OT-systemer

Sårbare og/eller utdaterte OT-systemer uten muligheter for sikkerhetsoppdatering kan for eksempel sikres ved å isolere dem helt fra internett, ved å «pakke dem inn» i sikre nettverkssegmenter med god tilgangsstyring, innføre overvåkning, fysisk sikring og andre sikkerhetsmekanismer. Det er vannverket som må vurdere hvilke sikkerhetstiltak som er hensiktsmessig i lys av lokale forhold og situasjoner. ISO 27019 gir sammen med standardene ISO 27001 og 27002 råd og veiledning på sikring av OT-systemer. Amerikanske NIST Special Publications Guide to Operational Technology (OT) Security er gratis og gir veiledning på sikring av OT-systemer.

Sikring av IT-systemer

Virksomheten bør innføre NSMs Grunnprinsipper for IKT-sikkerhet, kategori 1- og 2-tiltak for å sikre IT-systemene. Som en start kan virksomheten benytte grunnprinsippene som en sjekkliste for IT-sikkerheten. Inviter IT-driftsleverandøren til et møte der dere i fellesskap går igjennom listen over de viktigste sikkerhetstiltakene i kategori 1 og 2.

Dersom man heller ønsker å se til internasjonale standarder så gir ISO 27001 og 27002 til sammen et rammeverk for sikring av IT-systemer. Amerikanske NIST Cyber Framework er et gratis rammeverk med flere nyttige verktøy og veiledninger til arbeidet med å sikre IT-systemer.

6.5 Ressurser

NSM Grunnprinsipper for IKT-sikkerhet

Støtteprodukter - Nasjonal sikkerhetsmyndighet

Passordråd for personer og virksomheter - Nasjonal sikkerhetsmyndighet

Standard Norge | standard.no. ISO/IEC 27019:2024

CSF 2.0 Informative References | NIST

NIST Guide to Operational Technology (OT) Security

Helse- og kommuneCERT:

- OT-sjekk - Norsk helsenett
- https://www.nhn.no/tjenester/helsecert/nasjonalt-beskyttelsesprogram-nbp/anbefalte-sikkerhetstiltak/ot-sjekk
- https://www.nhn.no/tjenester/helsecert/nasjonalt-beskyttelsesprogram-nbp/webinarer

KraftCERT/InfraCERT

CERT-tjenester

CERT står for *Computer Emergency Response Team*. For drikkevannsforsyningen er det særlig responsmiljøene *Helse- og kommuneCERT* og *Kraft/InfraCERT* som er relevant. Disse responsmiljøene kan formidle informasjon om aktuelle cybertrusler og sårbarheter i vannsektoren, gi råd om sikring av IT- og OT-systemer samt håndtering av pågående cyberangrep. Helse- og kommuneCERT er gratis og krever kun medlemskap i Nasjonal beskyttelsesprogram (gratis).

6.6 Krysskobling

§ 6.Styringssystem for sikkerhet

§ 7. Risikostyring

7. Fysiske sikkerhetstiltak

7.1 Ingress

Virksomheten skal iverksette tiltak for fysisk sikkerhet. Tiltakene skal bidra til å opprettholde forsvarlig sikkerhet.

7.2 Krav

---

§ 11. Fysiske sikkerhetstiltak

En tilbyder av en samfunnsviktig tjeneste skal iverksette tiltak for fysisk sikkerhet for å opprettholde forsvarlig sikkerhet i nettverk og informasjonssystemer.

Fysiske sikkerhetstiltak skal minst omfatte

a. tiltak for å forhindre at uvedkommende får tilgang til lokasjoner og fysisk og teknisk infrastruktur som nettverk og informasjonssystemer benytter eller er avhengig av

b. tiltak for å identifisere og beskytte bygninger, rom og tilstøtende områder som har betydning for sikkerhetsnivået til nettverk og informasjonssystemer som understøtter den samfunnsviktige tjenesten

c. tiltak for å ivareta eksterne avhengigheter, herunder datakommunikasjon og strømtilførsel

d. tiltak for å avdekke hendelser med negativ virkning på sikkerheten i nettverk og informasjonssystemer.

7.3 Ordforklaring

Ord	Ordforklaring
Lokasjon	Lokasjoner er geografiske steder hvor systemer og utstyr står plassert.
Teknisk infrastruktur	Systemer, løsninger og plattformer for informasjonsflyt, -behandling og -lagring av data.
Fysisk infrastruktur	Til eksempel servere, kabler for elektronisk kommunikasjon, nettverksutstyr, adgangskontrollsystemer, kjøle- og ventilasjonsanlegg samt energiforsyning.

7.4 Hvordan oppfyllet kravet?

For å oppfylle kravet skal virksomheten, som minimum ha:

a. **tiltak for å forhindre at uvedkommende får tilgang til lokasjoner og fysisk og teknisk infrastruktur som nettverk og informasjonssystemer benytter eller er avhengig av**

Et enkelt tiltak å gjennomføre er avlåste rom. Nøkler har ulik sikringsklasse. Virksomheten må vurdere hva som er tilstrekkelig sikringsklasse for nøkler og adgangskontroll til lokasjoner. Andre tiltak er alarmsystemer, gjerder og overvåkning av lokasjoner. Se NSMs Grunnprinsipper for fysisk sikring. Disse bidrar til å sikre lokasjoner mot alminnelig kriminalitet.

b. **tiltak for å identifisere og beskytte bygninger, rom og tilstøtende områder som har betydning for sikkerhetsnivået til nettverk og informasjonssystemer som understøtter den samfunnsviktige tjenesten**

Det er viktig at virksomheten har oversikt over bygg, anlegg og fysisk infrastruktur som de digitale systemene er avhengige av og lokalisert i, og identifiserer sårbarhetene byggene, anleggene og infrastrukturen kan utgjøre. Lokasjonene kan være utsatt for naturhendelser (flom, storm, ras, skred) eller spredningsfare ved brann. Andre eksempler kan være nærhet til andre som lett kan få tilgang til områdene (innsyn, innbrudd, sabotasje, uhell) eller miljømessige og tekniske sårbarheter (feil i ventilasjon og kjøling, lekkasje). Disse sårbarhetene må håndteres, og typiske tiltak kan være forsterkede dører, vegger, tak og vinduer, brannsikring, eller plassering av nettverk og informasjonssystemer i flomsikre områder.

NSMs grunnprinsipper for fysisk sikring gir mange eksempler på konkrete sikringstiltak.

c. **tiltak for å ivareta eksterne avhengigheter, herunder datakommunikasjon og strømtilførsel**

Virksomheten skal, basert på risikovurderingen og kritikaliteten til systemene, vurdere konsekvensen av tap eller reduksjon i mobilkommunikasjon, internett og strømforsyning. Aktuelle tiltak er reserveløsninger som for eksempel strømaggregat, batteri, satellittkommunikasjon, alternative internettleverandører, nødstrøm og manuelle beredskapsrutiner.

d. **tiltak for å avdekke hendelser med negativ virkning på sikkerheten i nettverk og informasjonssystemer.**

Eksempel på tiltak er overvåkningssystemer med kamera med tilhørende sensorer som IR, termisk og bevegelse, alarmanlegg eller andre midler. Dette kan tidlig gi varsling om en pågående sikkerhetstruende hendelse. Kameraer og andre deteksjonsmidler bør plasseres på egnede steder. Ved valg av leverandør av overvåkings- og sikringssystemer bør virksomheten gjøre en vurdering av leverandørens sikkerhetsmessige skikkethet. Mattilsynet henviser til PST og NSMs sikkerhetsråd.

Helhetlig sikring

Det er viktig å se flere sikkerhetstiltak i en sammenheng. Man bør gjøre en vurdering av sikringsnivået på teknologiske sikringstiltak og se disse i sammenheng med de fysiske sikringstiltakene som er på plass. Alle sikringstiltakene skal til sammen oppnå et forsvarlig sikringsnivå. Det vil si at noen minimumstiltak må være på plass, mens ytterligere tiltak vil være et resultat av at risikovurderingen peker på for høy risiko og økt behov for sikring.

7.5 Ressurser

NSM Grunnprinsipper for fysisk sikring

Sikringshåndboka - Forsvarsbygg

Rapport229_2017_Sikring_av_vannforsyning_mot_tilsiktede_uonskede_hendelser.pdf

7.6 Krysskobling

§ 6 Styringssystem for sikkerhet

§ 7 Risikovurdering

§ 8 Risikohåndtering

§ 12 Sikkerhetstiltak for personell, første ledd bokstav a om administrative tiltak for adgangsbegrensning

§ 14 Oppfølgningsplikt

8. Personellsikkerhet

8.1 Ingress

Virksomheten skal etablere tiltak som sikrer at kun autentiserte og autoriserte brukere har tilgang til digitale systemer. Personellsikkerhet innebærer også at alt personell må ha tilstrekkelig kunnskap og innsikt i egen rolle i sikkerhetsarbeidet.

8.2 Krav

---

§ 12.Sikkerhetstiltak for personell

En tilbyder av en samfunnsviktig tjeneste skal iverksette nødvendige sikkerhetstiltak for ansatte, leverandører og oppdragstakere som kan få tilgang til virksomhetens nettverk og informasjonssystemer gjennom å sørge for

a. at adgang til lokaler og tilganger til nettverk og informasjonssystemer tildeles basert på roller, oppgaver, ansvar og tjenstlig behov, samt følge opp at personell ikke har flere tilganger enn nødvendig

b. at personell nevnt i leddet her er gjort kjent med relevante sikkerhetstiltak, at de har tilstrekkelig kompetanse innenfor sikkerhet og gis nødvendig opplæring ved behov.

Når et arbeidsforhold eller en tjeneste avsluttes, skal en tilbyder av en samfunnsviktig tjeneste sikre at den som slutter ikke lenger har tilgang til virksomhetens nettverk og informasjonssystemer.

8.3 Ordforklaring

Ord	Ordforklaring
Ansatte	Ansatte i virksomheten som har ansettelseskontrakt og der virksomheten er arbeidsgiver med styringsrett.
Leverandører	Virksomheter som har et kontraktsforhold til virksomheten og leverer en tjeneste eller et produkt til virksomheten.
Oppdragstakere	Virksomheter som utfører et oppdrag på vegne av virksomheten, eksempelvis en konsulent.

8.4 Hvordan oppfylle kravet?

For å oppfylle kravet skal virksomheten, som minimum:

iverksette nødvendige sikkerhetstiltak for ansatte, leverandører og oppdragstakere som kan få tilgang til virksomhetens digitale systemer ved å sørge for

a. **at adgang til lokaler og tilganger til nettverk og informasjonssystemer tildeles basert på roller, oppgaver, ansvar og tjenstlig behov, samt følge opp at personell ikke har flere tilganger enn nødvendig**

Virksomheten skal ha et system som sørger for at alt personell kun har tilgang til de IT- og OT-ressurser, samt fysiske rom, som kreves for å gjennomføre arbeidet. Tilganger må sjekkes, og evt. revideres, ved stillingsendringer og omorganiseringer. Med leverandører som skal ha tilgang til fysiske anlegg og rom, samt IT og OT-systemer, bør det inngås en sikkerhetsavtale der krav til etterlevelse av sikkerhetskrav inngår.

Når et arbeidsforhold eller en tjeneste avsluttes skal virksomheten sikre at den som slutter fratas tilgang til virksomhetens digitale systemer. Mattilsynet anbefaler å gjennomføre sluttsamtale og formidle hvilke krav til taushet som gjelder etter at arbeidsforholdet er avsluttet og hvor lenge denne plikten varer.

b. **at personell nevnt i leddet her er gjort kjent med relevante sikkerhetstiltak, at de har tilstrekkelig kompetanse innenfor sikkerhet og gis nødvendig opplæring ved behov.**

Virksomheten skal også sørge for at alt personell har tilstrekkelig kompetanse om digital sikkerhet og gis nødvendig opplæring ved behov.

Ledelse hvor god sikkerhetskultur og bevisstgjøring vektlegges er et viktig personellsikkerhetsmessig tiltak. Plikten til kunnskaps- og kompetansebygging samt opplæring er løpende slik at oppfriskningskurs og vedlikehold av kompetanse kan være nødvendig.

8.5 Ressurser

Innsiderisiko - NSM temarapport

NSM kurssenter - Nasjonal sikkerhetsmyndighet

8.6 Krysskobling

§ 6 Styringssystem for sikkerhet

§ 9.Organisatoriske sikkerhetstiltak

§ 7 Risikovurdering

§ 8 Risikohåndtering

9. Hendelseshåndtering og beredskap

9.1 Ingress

Virksomheten skal ha beredskapsplan og øve på gjennomføringen av denne.

9.2 Krav

---

§ 13.Hendelseshåndtering og beredskap

En tilbyder av en samfunnsviktig tjeneste skal ha en beredskapsplan for håndtering av hendelser og varsling etter § 17. Tilbyderen skal vurdere relevante beredskapstiltak og skjerping i eksisterende sikkerhetstiltak som raskt kan iverksettes ved behov.

Når tilbyderens nettverk eller informasjonssystem er utsatt for en hendelse, skal hendelsens karakter og omfang identifiseres. Tilbyderen skal iverksette nødvendige mottiltak og tiltak for å gjenopprette den sikre tilstanden i nettverk og informasjonssystemet.

En tilbyder av en samfunnsviktig tjeneste skal utarbeide, vedlikeholde og dokumentere beredskapsplaner og gjennomføre øvelser for å teste planverket og utvikle virksomhetens kompetanse til å håndtere hendelser.

9.3 Ordforklaring

Ord	Ordforklaring
Beredskapsplan	Plan for hvordan virksomheten skal forberede seg på, håndtere og følge opp hendelser.
Beredskapstiltak	Tiltak som bidrar til å redusere skadeomfang og konsekvenser ved hendelser. Disse kan være tekniske, personellmessige og fysiske.
Mottiltak	Et sikringstiltak som virker mot en bestemt fare eller trussel og reduserer virkningen av denne trusselen eller faren.
Øvelser	Planlagte og strukturerte tiltak som gjennomføres for å bygge kompetanse og erfaring for å styrke virksomhetens evne til å forebygge, motstå og håndtere hendelse.

9.4 Hvordan oppfylle kravet?

For å oppfylle kravet skal virksomheten, som minimum:

- Ha en fungerende backup (sikkerhetskopi av kritisk data). I praksis betyr dette at backup må testes innimellom så fremt det er praktisk mulig.
- Ha en beredskapsplan med forhåndsvurderte tiltak som kan iverksettes når det oppstår en hendelse. Beredskapsplanen skal gi nødvendig kontaktinformasjon og prosedyre for varsling til Mattilsynet og NSM, samt andre aktører, som for eksempel leverandører av CERT-tjenester.
- Gjennomføre øvelser. En øvelse kan adressere ulike tema og kan både være en teoretisk skrivebordsøvelse eller en praktisk øvelse. Hensikten med øvelser er dels å teste beredskapsplanen og eventuelt avdekke mangler, og dels å trene ledelse og personell slik at man ved reelle hendelser vet man hva man skal gjøre. Gjennomføringens hyppighet og metodevalg må vurderes i lys av proporsjonalitet og virksomhetens risikovurdering. Mattilsynet anbefaler minst årlig gjennomføring.

Lokale, regionale og nasjonale myndigheter kan sende varsler om økt beredskap. Når varslet omhandler digitale tjenester må vannverkseier være beredt til å iverksette nødvendige tiltak som opprettholder forsvarlig sikkerhet i digitale systemer. Mattilsynet anbefaler at virksomheten i beredskapsplanen også utarbeider rutiner og tiltak som kan iverksettes dersom et slikt varsel sendes.

9.5 Ressurser

Nasjonal sikkerhetsstrategi - regjeringen.no

Meld. St. 9 (2024–2025) - regjeringen.no

Sikkerhetskopier - Norsk helsenett

9.6 Krysskobling

§ 6 Styringssystem for sikkerhet

§ 7 Risikovurdering

§ 8 Risikohåndtering

10. Oppfølgingsplikt

10.1Ingress

Virksomheten skal sikre at leverandører og andre som utfører arbeid på vegne av virksomheten, følger kravene til forsvarlig sikkerhet. Hvis nødvendig skal virksomhetens sikkerhetstiltak, gjennom avtale, gjøres gjeldende for disse.

10.2 Krav

---

§ 14.Oppfølgingsplikt

En tilbyder av en samfunnsviktig tjeneste skal påse at leverandører og andre som utfører arbeid som kan påvirke sikkerheten i nettverk og informasjonssystemer og som utfører arbeid for eller på vegne av virksomheten, utfører arbeidet på en måte som gjør at kravene til forsvarlig sikkerhet overholdes.

En tilbyder av en samfunnsviktig tjeneste skal, gjennom avtale eller på annen egnet måte, gjøre sikkerhetstiltakene gjeldende overfor leverandører som nevnt i første ledd, i den grad det er nødvendig for å opprettholde et forsvarlig sikkerhetsnivå.

10.3 Ordforklaring

Ord	Ordforklaring
Påse	Synonymt med «sørge for» og innebærer et ansvar til å gjennomgående følge opp og verifisere at krav og tiltak etterleves.

10.4 Hvordan oppfylle kravet?

For å oppfylle kravet skal virksomheten, som minimum:

- Foreta en konkret og risikobasert vurdering av hver enkelt leverandør eller oppdragstaker. Dersom det er nødvendig, skal det inngås avtale med leverandør eller oppdragstaker om at disse omfattes av de relevante sikkerhetstiltakene.
- Sikre løpende oppfølgning av leverandører, underleverandører, konsulenter, oppdragstakere og andre parter så lenge virksomheten har et samarbeid eller

forbindelse med dem.

Virksomheten har en påseplikt overfor leverandør

Med mindre leverandøren selv er omfattet av digitalsikkerhetsforskriften etter § 1 eller gjennom enkeltvedtak etter § 4, gjelder ikke digitalsikkerhetsloven- og forskriften direkte for leverandøren.

Leverandørers plikt til å etterleve krav i digitalsikkerhetsforskriften bør derfor reguleres i kontrakt eller sikkerhetsavtale mellom virksomhet og leverandør. Leverandørens etterlevelse skal kontrolleres av virksomheten som en del av leverandøroppfølgingen.

For å være i samsvar med påseplikten må virksomheten sørge for at krav etter digitalsikkerhetsforskriften er tatt med:

- i utarbeidelse av konkurransegrunnlaget
- i eventuelle forhandlinger før virksomheten skriver kontrakt med leverandør, konsulent eller aktør
- i kontrakten eller egen sikkerhetsavtale når kontrakten signeres

Virksomheten skal løpende følge opp og/eller kontrollere at forskriften etterleves av leverandør, konsulent eller annen partner

- under hele avtaleperioden, det kan gjøres i årlig møte, eller som revisjon eller kontroll av leverandøren.
- ved avslutning av kontrakten, det kan gjøres i et sluttmøte der man går igjennom kontraktsvilkårene og sammen sjekker at avslutningen ikke introdusere risiko, men er i samsvar med forskriftens krav slik de framgår av avtalen.

Påseplikten bør ha en egen rutine i virksomhetens styringssystem, hvis relevant kan det utpekes en ansvarlig for leverandøroppfølgning. Det kan være et eget dokument som beskriver hva påseplikten er og hvordan den skal følges opp.

Behovsstyrt leverandørtilgang

Trenger leverandører 24/7-tilgang alle dager i året? Det er ulike tekniske løsninger for leverandørtilgang, eks. VPN, Team Viewer. Tilgang kan gis når det trengs.

Fire råd fra Kommune- og helseCERT:

- Ha avklarte ansvarsområder så du vet hvem som gjør hva
- Ha en formell og tydelig driftsavtale med leverandør
- Kartlegg angrepsflaten (sårbarheter) og fjerntilganger
- Gjennomfør revisjoner eller kontroller, jf. dsf § 14

10.5 Ressurser

Kvalitetsordning for leverandører som håndterer IKT-hendelser - Nasjonal sikkerhetsmyndighet

Riktige og gode krav til IKT-tjenesten og til leverandør - Nasjonal sikkerhetsmyndighet

10.6 Krysskobling

§ 6 Styringssystem for sikkerhet

§ 7 Risikovurdering

§ 8 Risikohåndtering

11. Hendelseshåndtering og beredskap

11.1 Ingress

Virksomheten skal varsle Mattilsynet og NSM om hendelser som har negativ innvirkning på sikkerheten i digitale systemer når hendelsen har betydelig innvirkning på vannverkets evne til å opprettholde drikkevannsforsyningen.

11.2 Krav

---

§ 17.*Varslingsplikt*

Et varsel etter digitalsikkerhetsloven §§ 8 og 11 skal sendes til tilsynsmyndigheten med kopi til Nasjonalt kontaktpunkt. Varselet skal sendes senest innen 24 timer etter at en tilbyder av en samfunnsviktig tjeneste fikk kjennskap til hendelsen. Varselet skal inneholde informasjon om

a. tilbyderens navn og kontaktinformasjon

b. berørt tjeneste

c. hendelsen, herunder mulige årsaker og konsekvenser

d. antall berørte brukere

e. hendelsens virkninger i andre land.

Informasjonen i varselet skal oppdateres innen 72 timer.

Innen en måned fra varsel som nevnt i første ledd er sendt, skal tilbyderen gi tilsynsmyndigheten en hendelsesrapport. Hendelsesrapporten skal inneholde oppdatert informasjon om forhold som nevnt i første ledd og hvilke avhjelpende tiltak som er iverksatt.

Tilsynsmyndigheten kan kreve statusoppdateringer og de opplysningene som er nødvendige for å utføre pålagte oppgaver.

11.3 Ordforklaring

Ord	Ordforklaring
Varsel	Kort informasjon om noe som akkurat har inntruffet, før man har full oversikt over situasjonen.
Nasjonalt kontaktpunkt	Her: Nasjonal sikkerhetsmyndighet NSM.
«Betydelig innvirkning»	Her: En skjønnsmessig vurdering hvor blant annet antallet brukere som påvirkes, hendelsens varighet og størrelsen på det geografiske området som berøres skal vektlegges, jf. digitalsikkerhetsloven § 8.

11.4 Hvordan oppfylle kravet?

For å oppfylle kravet skal virksomheten varsle Mattilsynet med kopi til NSM om:

- Hendelser som gir driftsforstyrrelser eller konsekvenser for leveringen av helsemessig trygt drikkevann dersom disse skyldes hendelser i virksomhetens digitale systemer. Slike hendelser skal varsles til Mattilsynet med kopi til NSM innen 24 timer. Varsel skal sendes på skjema *Varsel om alvorlig hendelse etter digitalsikkerhetsloven*
- Innen 72 timer skal virksomheten gi Mattilsynet, med kopi til NSM, oppdatert informasjon om hendelsen.
- Innen 1 måned etter at første varsel ble sendt, skal virksomheten sende Mattilsynet en rapport som oppsummerer hendelsen og omtaler tiltak som er iverksatt for å redusere og forebygge skade.

Varsling av hendelser

Hendelser som virker betydelig inn på/har konsekvenser for vannverkets evne til å levere helsemessig trygt drikkevann skal varsles. Eksempel på hendelser som skal varsles:

- Feilet programvareoppdatering med konsekvens for drikkevannslevering eller drikkevannskvalitet
- Redundant system som feiler selv om det ene systemet virker
- Datainnbrudd
- Naturhendelser med brudd på tjenesteleveransen eller -kvaliteten
- Fysisk innbrudd med brudd på tjenesteleveransen eller -kvaliteten

Dersom du er i tvil, bør du varsle Mattilsynet med kopi til NSM heller en gang for mye enn en gang for lite.

Mattilsynet anbefaler virksomhetene å varsle CERTer de har samarbeid med om hendelser så snart som mulig (uten ugrunnet opphold). Terskelen for å varsle samarbeidende CERT bør være lav. CERTer bidrar operativt i hendelsesrådgivning og kan raskt dele informasjon i sine kontaktnettverk. Informasjonsdeling er viktig for å forhindre at hendelsen sprer seg til andre virksomheter.

Varslingsplikt etter drikkevannsforskriften

Ved mistanke om overskridelse av grenseverdier, eller ved overskridelser av tiltaksgrenser som kan utgjøre helsefare, skal vannverkseier straks varsle abonnentene og Mattilsynet, jf. drikkevannsforskriften § 23 og § 24.

Bestemmelsene er forstått dithen at det ved mistanke om en uønsket digital hendelse også vil være grunn til mistanke om utrygt drikkevann, og at varslingsplikten dermed aktualiseres.

Varslingsplikten etter drikkevannsforskriften gjelder alle vannverk, også de som faller under terskelverdien i digitalsikkerhetsforskriften. Meldeplikten gjelder der det er grunn til mistanke om utrygt drikkevann eller manglende leveringssikkerhet[1].

11.5 1Ressurser

Skjema for Varsel om alvorlig hendelse etter digitalsikkerhetsloven

Nasjonalt rammeverk for håndtering av digitale angrep og cyberhendelser - Nasjonal sikkerhetsmyndighet

Helse- og KommuneCERT

KraftCERT/InfraCERT

11.6 Kobling til annet regelverk

Matloven § 6 pålegger virksomhetene å umiddelbart varsle tilsynsmyndigheten (Mattilsynet) dersom det foreligger grunn til mistanke om helseskadelige næringsmidler.

Drikkevannsforskriften § 23

Drikkevannsforskriften § 24.

1.6 Krysskobling

§ 6 Styringssystem for sikkerhet

§ 12 Sikkerhetstiltak for personell

§ 11 Varslingsplikt