Veileder i ledelsessystem for informasjonssikkerhet i sektor for høyere utdanning og forskning

Basert på ISO/IEC 27001:2022

Versjon	Dato	Kommentar
3.0	*2021-03-22*	*Foreløpig utgave etter full gjennomgang av v2.2 (2017)*
3.0.1	*2024-10-22*	*Oppdatert referanser*

Forord

Universiteter og høgskoler er pålagt å innføre et ledelsessystem for informasjonssikkerhet. Dette følger både av lovgivningen som gjelder i universitets- og høgskolesektoren og av nye krav som Kunnskapsdepartementet stiller til virksomhetene i tildelingsbrevet. Ledelsessystemet skal være en del av virksomhetenes generelle system for kvalitetsstyring og internkontroll.

Denne veilederen er ment å være til hjelp ved innføring og videreutvikling av ledelsessystem for informasjonssikkerhet, spesielt tilpasset sektor for høyere utdanning og forskning. Innholdet baserer seg på anerkjente standarder for statsforvaltningen (ISO/IEC 27001/02: 2022) og ivaretar de kravene som lovverket stiller til slike ledelsessystemer.

Formål og målgruppe

Formålet er å bidra til at sektorens virksomheter forvalter sine informasjonsverdier på en sikker og profesjonell måte. Veilederen retter seg mot toppledere, mellomledere og ansatte med ansvar for informasjonssikkerhet. Etableringen av et ledelsessystem er nevnt som et sentralt tiltak i arbeidet med informasjonssikkerhet og personvern i Kunnskapsdepartementets policy for informasjonssikkerhet og personvern i sektoren.

Lokal tilpasning

Virksomheter som baserer sitt arbeid med informasjonssikkerhet på denne veilederen må likevel tilpasse ledelsessystemet til lokale forhold. Uten en slik tilpasning vil det være vanskelig å gjøre ledelsessystemet til sitt eget og det kan bli utfordrende å implementere og vedlikeholde ledelsessystemet.

Videreutvikling av denne veilederen

Videreutvikling av ledelsessystem for informasjonssikkerhet vil være en prioritert oppgave for rådgivningstjenesten i sektorens cybersikkerhetssenter for forskning og utdanning (eduCSC). Veilederen vil bli oppdatert ved relevante endringer i lov- og regelverk, føringer fra direktoratet for høyere utdanning og kompetanse (HK-dir) og departement, og sektorens økende modenhet på området.

Kurs og bistand

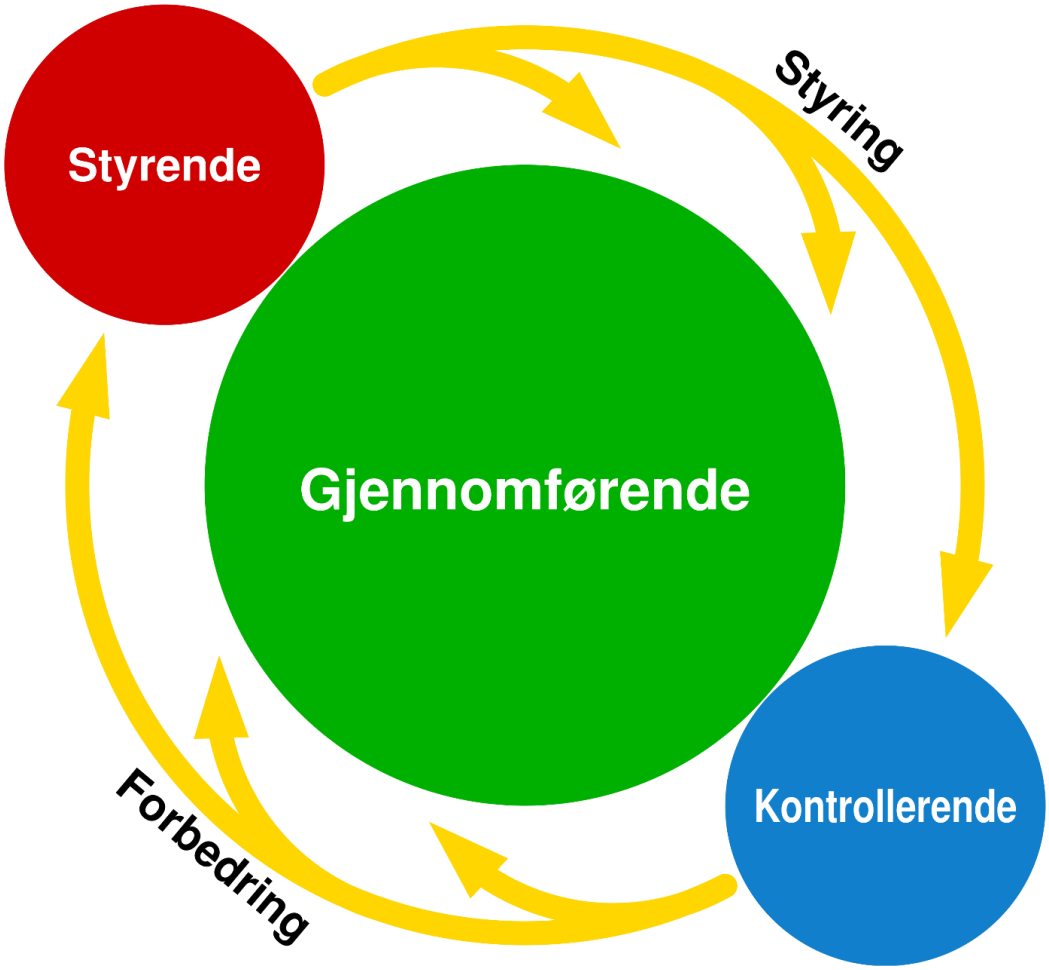
EduCSC tilbyr virksomhetene bistand til innføring, videreutvikling og revisjon av ledelsessystemet. Det vil også bli utarbeidet og gjennomført kurs i innføring, vedlikehold og drift av ledelsessystemet. Kurset vil være spesielt tilpasset universiteter og høgskoler.

Ta gjerne kontakt med kontakt@sikt.no dersom du har spørsmål i forbindelse med informasjonssikkerhet eller ledelsessystem.

Innhold

Ledelsessystemets struktur, tittel og innledning

Forslaget til ledelsessystem er inndelt i følgende hoveddeler: en styrende del, en gjennomførende del og en kontrollerende del. Hoveddelene omhandler de tre kjerneaktivitetene som et systematisk og planlagt informasjonssikkerhetsarbeid består av. Hver hoveddel består av (a) kommentarer til de dokumenter og oppgaver som inngår i et ledelsessystem for informasjonssikkerhet og (b) forslag til utforming av de viktigste dokumentene og arbeidsredskapene som inngår i ledelsessystemet. Til hvert av forslagene er det laget maler som virksomhetene kan anvende i arbeidet med etableringen av sine egne ledelsessystemer. Lenker til malene finnes fortløpende i teksten (nederst under hver deloverskrift).



Hoveddokumentet bør ha en tittel som dekker hele området, som «Ledelsessystem for informasjonssikkerhet ved . . . ». Tittelsiden bør tydelig uttrykke når den aktuelle revisjonen er vedtatt, eventuelt med versjonsnummer. Den kan med fordel også opplyse om at innholdet er basert på ISO/IEC 27001:2022.

Innledningskapittelet bør henvende seg til et bredest mulig internt publikum og bør inneholde to hovedpunkter:

1. Definisjon av informasjonssikkerhet som forvaltning av virksomhetens immaterielle verdier: informasjon, omdømme, tillitsrelasjoner, kunnskap, rettigheter, prosesser og kultur.

2. Oversikt over krav til arbeidet med informasjonssikkerhet: informasjonsforvaltning, lovpålagte krav og forventninger fra HK-dir og Kunnskapsdepartementet.

Del 1 – styrende dokumenter

Ledelsessystemets første hoveddel inneholder styrende dokumenter som uttrykker ledelsens føringer for virksomhetens arbeid med informasjonssikkerhet. De styrende dokumentene omfatter beskrivelser av:

- Virkeområdet til ledelsessystemet («scope»)
- Sikkerhetsmål
- Sikkerhetsstrategi
- Kriterier for akseptabel risiko
- Sikkerhetsorganisering

1.1 Virkeområdet til ledelsessystemet

Virkeområdet beskriver hvilke deler av organisasjonen, tekniske ressurser og informasjonsverdier som inngår i ledelsessystemet. Hensikten med beskrivelsen er ikke bare å definere hva og hvem som omfattes av arbeidet med informasjonssikkerhet, men kan også tjene den pedagogiske hensikten å vise at informasjonssikkerhet er et bredt arbeidsfelt som krever et visst minimum av ressurser og fokus.

I lenkene nedenfor skisseres to forslag til virkeområde – det første mer omfattende enn det andre. Virksomhetene må selv velge hvilket forslag de ønsker å basere seg på. Mindre virksomheter vil trolig kunne basere seg på det enkleste forslaget.

Uavhengig av hvilket forslag som velges, er det viktig å være oppmerksom på at alle virksomhetene skal ha dokumentasjon av datanettverk (og IT-ressurser i nettverket) som behandler personopplysninger. Oversikter over de IT-ressursene som inngår i ledelsessystemet bør derfor ivaretas gjennom en oversikt som viser IT-systemer og relasjonene mellom dem. I tillegg skal det dokumenteres hvilke IT-systemer som driftes av virksomheten, databehandlere eller andre eksterne aktører.

Dokumentasjonen skal gi en overordnet oversikt over sikringstiltak i datanettverket, for eksempel soneinndelinger, plassering av brannmurer, VLAN, DMZ, osv.

Virksomhetene skal også lage en oversikt over informasjonsverdier som de er ansvarlige for. Oversikten bør inneholde en klassifisering av informasjonen som behandles i de ulike IT-systemene (se også kapittel 2.3, «Verdioversikt»).

1.2 Sikkerhetsmål

Sikkerhetsmålene skal beskrive hva ledelsen ønsker å oppnå med informasjonssikkerhetsarbeidet, og vil dermed kunne fungere som en rettesnor for arbeidet og danne grunnlag for senere evaluering.

I tillegg til at sikkerhetsmålene skal gi retning til informasjonssikkerhetsarbeidet, kan de fungere som pedagogiske hjelpemidler: Sikkerhetsmålene kan fortelle resten av virksomheten at arbeidet skal prioriteres og hvorfor det er viktig.

Når det gjelder elektronisk behandling av personopplysninger og personopplysninger som inngår i manuelle personregistre, er virksomhetene pålagt å sørge for *tilstrekkelig informasjonssikkerhet* (Jf. spesielt artikkel 5 og 32 i personvernforordningen). Definisjonen av tilstrekkelig vil avhenge av informasjonens art og omfang, risikonivå og hva som til enhver tid er teknisk og økonomisk mulig. Tilsvarende krav gjelder for andre typer informasjonsverdier, for eksempel økonomi- og regnskapsdata.

Sikkerhetsmålene bør gjennomgås og eventuelt revideres årlig i forbindelse med ledelsens gjennomgang.

1.3 Sikkerhetsstrategi

Sikkerhetsstrategien skal uttrykke hva ledelsen mener er viktigst å gjøre for at sikkerhetsmålene skal bli oppfylt i den daglige håndteringen av virksomhetens informasjonsverdier. Strategien skal inneholde en oversikt over de grunnleggende prioriteringer som virksomhetens ledelse foretar for å følge opp og realisere sikkerhetsmålene.

Det er viktig å være oppmerksom på at ledelsen gjennom sikkerhetsstrategien forplikter seg til å bruke ressurser på arbeidet med informasjonssikkerhet. De prioriteringene som strategien uttrykker må derfor avspeile seg i det øvrige plan- og strategiarbeidet, og i interne budsjettprosesser.

Sikkerhetsstrategien bør gjennomgås og eventuelt revideres årlig i forbindelse med ledelsens gjennomgang.

1.4 Kriterier for akseptabel risiko

Kriterier for akseptabel risiko vil være overordnede og uttrykke virksomhetens hovedkrav til sikring av informasjonsverdier. Kriterier for akseptabel risiko skal fungere som et grunnlag for de som gjennomfører risikovurderinger.

Hvilke kombinasjoner av sannsynlighet og konsekvensnivå som anses som akseptable uttrykkes i en matrise, eventuelt supplert med en kort beskrivelse av hva som aksepteres av brudd på konfidensialitet, integritet og tilgjengelighet.

Erfaringen til rådgivningstjenesten i eduCSC samsvarer godt med sektorens.

1.5 Sikkerhetsorganisering

Sikkerhetsorganiseringen fordeler myndighet, ansvar og oppgaver mellom aktører som skal jobbe med informasjonssikkerheten ved virksomheten – fra toppledelsen og ut til sluttbrukerne (ansatte, studenter, gjester, osv.).

Det er viktig at beskrivelsen av sikkerhetsorganisasjonen er tydelig. Dette betyr at beskrivelsen skal gi klare svar på tre hovedspørsmål:

1. Hvem inngår i sikkerhetsorganisasjonen?
2. Hva har hver enkelt aktør som inngår i sikkerhetsorganisasjonen ansvaret for?
3. Hvilke konkrete oppgaver skal hver enkelt aktør utføre?

Mange universiteter og høgskoler har opprettet et hendelseshåndteringsteam («Incident Response Team» - IRT). Hovedoppgavene til IRT er å avdekke, håndtere og forebygge tekniske sikkerhetsbrudd. IRT jobber fortrinnsvis på eget mandat fra toppledelsen, men rollen må like fullt beskrives som en del av sikkerhetsorganisasjonen.

Avdelinger eller enheter kan ha tverrgående ansvar for informasjonssikkerheten på et bestemt område. Med dette menes for eksempel at avdelinger i sentraladministrasjonen kan være eiere av IT-systemer eller tjenester som også anvendes i andre avdelinger eller enheter ved virksomheten (for eksempel administrative fellessystemer). Avdelinger eller enheter med et slikt ansvar har som oppgave å vurdere behovet for sikringstiltak som omfatter alle som anvender «deres» systemer eller tjenester.

Enheter som IT-avdeling og eiendomsavdeling har et særlig tverrgående ansvar for informasjonssikkerheten når det gjelder IT-infrastruktur og fysisk infrastruktur. Myndighet, ansvar og oppgaver til lederne i disse avdelingene behandles derfor særskilt i forslaget.

Virksomheten kan velge å opprette et informasjonssikkerhetsforum for å koordinere arbeidet med informasjonssikkerhet på tvers av hele organisasjonen. Oppgavene til et slikt forum kan legges til et allerede eksisterende organ ved virksomheten, forslaget må i så fall tilpasses dette.

Rådgivningstjenesten i eduCSC kan bistå i arbeidet med den lokale tilpasningen av sikkerhetsorganiseringen.

Del 2 – gjennomførende dokumenter

Etter hvert som ledelsessystemet slår rot i organisasjonen, vil det ta opp i seg en økende mengde gjennomførende dokumenter. Noen av disse vil være nye dokumenter skrevet på grunnlag av føringene i de styrende dokumentene. Andre vil være tilpasninger av dokumenter som allerede eksisterer, men som innlemmes i ledelsessystemet etter en eventuell tilpasning.

Det kan være nyttig å knytte NSMs grunnprinsipper for IKT-sikkerhet opp mot underkapitlene her:

1. *Identifisere og kartlegge* — 2.3 Verdioversikt, 2.5 Risikostyring
2. *Beskytte og opprettholde* — 2.6 Robusthetsarbeid, 2.8 Kontinuitetsplaner
3. *Oppdage* — 2.5 Risikostyring, 2.6 Robusthetsarbeid, 2.9 Øvelser, 2.10 Revisjon
4. *Håndtere og gjenopprette* — 2.7 Hendelseshåndtering, 2.4 Avvikshåndtering

2.1 Grunnleggende dokumenter

2.1.1 Trusselbilde

Som et supplement til styringssignaler fra ledelsen om hva man ønsker å oppnå med sikkerhetsarbeidet er det nødvendig å ha kjennskap til trusselsituasjonen. På ulike detaljnivåer er det viktig at ledelse, CISO og hendelseshåndteringsteam holder seg løpende oppdatert på dette området. Rapporter om trusselbildet utgis regelmessig av flere aktører både nasjonalt og internasjonalt, inkludert Nasjonal sikkerhetsmyndighet (NSM) og Politiets sikkerhetstjeneste (PST). På mer operativt nivå videreformidler eduCSC løpende varsler til hendelseshåndteringsteamene i sektoren og legger til rette for kunnskapsdeling både med og mellom disse.

2.1.2 Overordnet risikovurdering for virksomheten

Det stilles lovkrav til risikovurdering ved behandling av spesifikke typer informasjon; dette behandles i kapitler om risikostyring nedenfor. Imidlertid er det både anbefalt beste praksis og en forutsetning for å oppfylle alle krav i ISO 27001 at det også foreligger en risikovurdering av virksomheten på overordnet nivå. Hensikten med denne er å avdekke og vurdere hvilke risikoer som truer virksomhetens evne til å oppnå sine målsetninger. Dette inkluderer eksterne forhold som påvirker denne måloppnåelsen, deriblant regulatoriske forhold og forholdet til eksterne parter.

En overordnet risikovurdering behøver ikke følge samme rammeverk som risikovurdering av enkeltområder, ettersom både formål og oppfølging vil være annerledes. Resultatet av en slik risikovurdering vil være til nytte ved den lokale tilpasningen av virksomhetens ledelsessystem.

2.2 Planmessig arbeid med informasjonssikkerhet

Den løpende oppfølgingen av ledelsessystemet er den mest sentrale oppgaven til informasjonssikkerhetsleder (CISO). Dette kapitlet beskriver verktøy for å gjøre dette systematisk og planmessig. Ansvaret for at ledelsessystemet fungerer etter hensikten er imidlertid ledelsens ansvar, og beskrives nærmere nedenfor i del 3, kontrollerende dokumenter.

2.2.1 Årshjul

Hvordan gjentagende oppgaver skal fordeles ut over året bør dokumenteres i et årshjul. Dersom ledelsens gjennomgang gjennomføres årlig vil det være naturlig å sørge for at CISO får samlet inn oversikt over status for alle aktivitetsområder for presentasjon til ledelsen. Dette vil kunne legge føringer på når ulike aktiviteter bør gjennomføres. Tilsvarende bør årshjulet ta hensyn til når viktige ressurspersoner har begrenset kapasitet på grunn av andre årlig gjentagende oppgaver.

2.2.2 Gjeldende årsplan (kapitler nevnes enkeltvis nedenfor)

Årsplanen inneholder konkrete aktiviteter og milepæler for arbeidet med informasjonssikkerhet for inneværende år. Årshjulet definerer en mal for årsplanen, som fylles med innhold som skal bidra til å oppfylle årsmålsetningene vedtatt i ledelsens gjennomgang. CISO vil normalt presentere et forslag til ny plan for behandling og vedtak, og kan eventuelt gis mandat til å supplere med detaljer i ettertid.

En årsplan inneholder både en samlet oversikt over årsmålsetningene for informasjonssikkerhetsarbeidet og særskilte planer for gjennomføring av de faste oppgavene i ledelsessystemet.

2.3 Verdioversikt

Mange underliggende aktiviteter i gjennomførende del forutsetter oversikt over hvilke informasjonsverdier virksomheten har, hvor viktige de er for virksomheten og hvilken beskyttelse de har behov for. En komplett oversikt forutsetter involvering fra alle informasjonseiere. Rollen til informasjonssikkerhetsansvarlig vil på dette området i hovedsak være å samordne ulike innspill og påse at oversikten holdes oppdatert.

2.3.1 Retningslinjer for verdioversikt

Verdioversikten må inneholde:

- ansvarsforhold
- hvor informasjonen befinner seg
- vurdering av virksomhetskritikalitet (setter krav til integritet og tilgjengelighet, se kapittel 2.8 under)
- vurdering av sensitivitet (setter krav til konfidensialitet)
- peker til eventuelle risikovurderinger

Ved etablering av en verdioversikt kan man benytte seg av eksisterende materiell som arkivplaner, systemoversikter og tilsvarende. For vår sektor anbefales å benytte sektorstandard for klassifisering av informasjon[1] (under revisjon). Her defineres fargemerkede klasser som beskriver både hvordan den klassifiserte informasjonen skal beskyttes og hvordan den kan benyttes.

2.3.2 Retningslinjer for dokumentasjon av bruk av personopplysninger

Personopplysningsloven (GDPR) setter en del krav til dokumentasjon av behandling av personopplysninger. Det vil være naturlig å koordinere denne oversikten («protokoll») med verdioversikten. Personvernombudet har ansvar for å kontrollere at denne er oppdatert. Når virksomheten opptrer som databehandler er kravene noe mindre omfattende enn når man er behandlingsansvarlig.

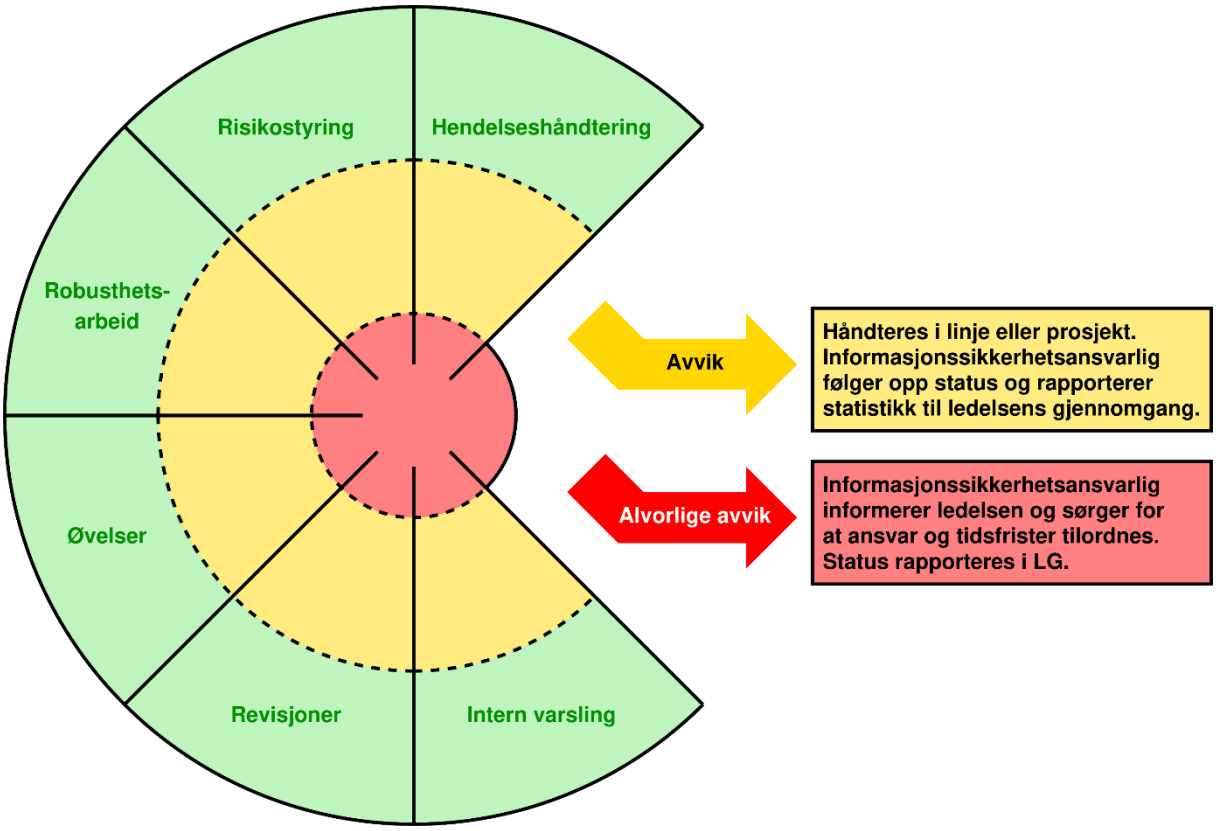
Mal for behandlingsansvarliges protokoll fra Datatilsynet:
https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/forordningen/artikkel-30_protokoll-behandlingsansvarlig.xlsx

Mal for behandlingsansvarliges protokoll fra Datatilsynet:
https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/forordningen/artikkel-30_protokoll-databehandler.xlsx

2.4 Avvikshåndtering

Det finnes flere ulike definisjoner av begrepet *avvik* i forskjellige kontekster. Det vil for eksempel være forskjell mellom betydningen «mangelfull etterlevelse av rutiner» og «sensitive personopplysninger på avveier». I dette dokumentet vil vi skille mellom avvik i bred forstand og *alvorlige avvik* som innebærer en situasjon som er i strid med ledelsens vedtatte akseptkriterier, og dermed krever særskilt oppfølging.

[1] https://cms.sikt.no/sites/default/files/2023-02/Sektorstandard_klassifisering_av_informasjon%20%281%29.pdf



Informasjon om potensielle avvik vil komme fra flere ulike kilder. Alle prosesser som har som oppgave å avdekke avvik eller har dette som en forventet sideeffekt bør ha definerte kriterier for å vurdere hvilke saker som utgjør avvik, og hvilke av disse som er så alvorlige at de skal eskaleres.

Vi anbefaler at den som er ansvarlig for informasjonssikkerheten (for eksempel CISO):

- Varsler ledelsen når alvorlige avvik avdekkes.
- Vedlikeholder en oversikt over alvorlige avvik, med ansvarlige og tidsfrister.
- Oppsummerer tilstanden til ledelsens gjennomgang, og om denne indikerer at ledelsessystemet bør justeres.

2.4.1 Intern varsling

Alle som er omfattet av ledelsessystemets virkeområde skal melde fra når de oppdager avvik. Dette er viktig for å oppdage problemer og årsakene til dem så tidlig som mulig, og dermed muliggjøre målrettede tiltak for å utbedre situasjonen.

Størrelsen på virksomheten vil legge sterke føringer på hvordan intern varsling håndteres. Som et minimum anbefaler vi følgende:

- Etablere et lett tilgjengelig system for varsling. Det bør vurderes hvorvidt varsling skal kunne skje anonymt.

- Etablere retningslinjer for om varsler skal regnes som avvik. Ansvarlig for dette beskrives også i sikkerhetsorganisasjonen.

- Etablere rutine for protokollføring av avvik og overlevering til linje eller informasjonssikkerhetsansvarlig for videre oppfølging. Slik oppfølging kan omfatte endringer av eller innskjerpinger i eksisterende rutine, eller iverksetting av tekniske sikringstiltak.

- Vedlikeholde oversikt over status for oppfølging av avvik. Informasjonssikkerhetsansvarlig må ha tilgang til denne oversikten for å kunne rapportere årsstatus til ledelsens gjennomgang.

- Etablere retningslinjer for å vurdere om et avvik skal regnes som alvorlig, og hvordan slike skal eskaleres.

Et slikt system for intern varsling kan samkjøres på tvers av flere fagområder, som HMS og personvern. Merk at ved brudd på sikkerheten til personopplysninger kan virksomheten i henhold til personopplysningsloven (GDPR) ha plikt til å varsle Datatilsynet, behandlingsansvarlig og de enkeltpersoner som berøres av sikkerhetsbruddet.

2.5 Risikostyring

Risikostyring er en sentral del av informasjonssikkerhetsarbeidet og forutsettes inkludert i ledelsessystemet alt fra etableringen.

2.5.1 Retningslinjer for risikovurderinger

For å sørge for at arbeidet blir effektivt, dekkende og sammenlignbart på tvers av områder er det viktig å etablere faste retningslinjer for gjennomføring av risikovurderinger. Disse må inneholde en detaljering av hvordan ledelsens akseptkriterier skal implementeres, i form av skalaer for sannsynlighet og konsekvens.

2.5.2 Plan for gjennomføring av risikovurderinger

Årsplanen for informasjonssikkerhetsarbeidet skal inneholde oversikt over planlagte risikovurderinger. I tillegg skal det foretas risikovurderinger i forkant av større planlagte endringer og ved andre hendelser som har betydning for informasjonssikkerheten.
Informasjonssikkerhetsansvarlig skal følge opp planen og rapportere status for gjennomføring til ledelsen.

2.5.3 Arkiv over gjeldende risikovurderinger

Informasjonssikkerhetsansvarlig skal sørge for at det finnes et oppdatert arkiv over alle gjeldende risikovurderinger. Arkivløsningen må ivareta behovet for skjerming av innholdet, siden risikovurderinger ofte vil dokumentere virksomhetens sårbarheter.

2.5.4 Oppfølging

Avdekkede risikoer med rødt nivå (uakseptabelt etter ledelsens akseptkriterier) i systemer eller tjenester som er i drift utgjør alvorlige avvik. Disse bør følges opp i den felles prosessen for alvorlige avvik beskrevet i kapittel 2.4.

Øvrige røde avvik, gule avvik, samt forbedringsforslag knyttet til risikoelementer med akseptabelt risikonivå (grønn) forutsettes løst i linje- eller prosjektorganisasjonen. Informasjonssikkerhetsansvarlig bør følge opp dette arbeidet på overordnet nivå.

Ved fornyet risikovurdering av et område hvor nye tiltak er gjennomført er det viktig å vurdere i hvilken grad tiltakene har hatt den tilsiktede effekten.

2.6 Robusthetsarbeid

Vi definerer begrepet robusthet som evnen til å minimere uheldige konsekvenser som følge av uønskede endringer i omgivelsene. Dette kan oppnås på flere måter: å motstå eller tåle påvirkningen, å ha evnen til å kunne gjenopprettes etter påvirkningen eller å kunne tilpasse seg denne.

2.6.1 Retningslinjer for robusthetsarbeidet

Robusthetsområdet er det feltet hvor informasjonssikkerhetsarbeidet i størst grad berører den løpende driften av systemer og tjenester, og retningslinjer på området spenner fra overordnede arkitekturprinsipper til operative rutiner for spesifikke systemer. I kontekst av ledelsessystemet for informasjonssikkerhet er de viktigste oppgavene å koordinere de overordnede føringene på tvers av virksomheten, og å sørge for at de mer spesifikke rutinene er tilgjengelige, oppdaterte og relevante.

Eksempler på områder hvor man med fordel kan ha felles prinsipper eller rutiner er:

- Definerte autoritative kilder for data som gjenbrukes i mange systemer og hvilke API de er tilgjengelige gjennom
- Prinsipper for redundans og grunnsikring (for eksempel Uninetts UFS-er om «Sikring av fysisk infrastruktur»)
- Rutiner for sikkerhetsoppdateringer
- Rutiner for oppretting og avslutning av brukerkontoer
- Rutiner for endringshåndtering (*change management*) og konfigurasjonsstyring
- Rutiner for backup og logging
- Rutiner for sårbarhetsskanning og penetrasjonstesting

2.6.2 Oversikt over etablerte sikringstiltak

For å dokumentere eksisterende sikringstiltak og oppdage eventuelle mangler kan man fylle ut en «anvendelighetserklæring» (engelsk: *Statement of Applicability, SOA*) basert på tillegg A til NS-ISO/IEC 27001:2022. En slik erklæring skal dokumentere hvilke tiltak som er i iverksatt, og om noen bevisst er utelatt skal begrunnelsen dokumenteres her. Anbefalinger om beste praksis for hvert av punktene i denne finnes i ISO/IEC 27002:2022. På et mer detaljert nivå kan man også benytte anerkjente standarder som *CIS Critical Security Controls*[2] eller *NSMs grunnprinsipper for IKT-sikkerhet*[3].

2.6.3 Dokumentasjon over systemer og avhengigheter

Informasjonssystemer har ofte en høy grad av kompleksitet, der det finnes avhengigheter mellom ulike systemer. For å unngå at et system feiler som følge av problemer i et annet må slike

[2] https://www.cisecurity.org/controls/
[3] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/

avhengigheter kartlegges og dokumenteres. Slik dokumentasjon vil utgjøre grunnlaget for flere prosesserer innenfor sikkerhetsarbeidet, inkludert kontinuitetsplanlegging, hendelseshåndtering og endringshåndtering.

2.7 Hendelseshåndtering

2.7.1 Retningslinjer for hendelseshåndtering

Hendelseshåndteringsfunksjonen skal ha et koordinert mottaksapparat for varsler fra ulike interne og eksterne kilder. Det skal finnes rutiner for å vurdere hvorvidt et varsel utgjør en sikkerhetshendelse og kriterier for eskalering av enkeltsaker som krever utvidede fullmakter og/eller varsling til virksomhetsledelsen.

Virksomheter over en viss størrelse bør ha et formalisert hendelseshåndteringsteam (IRT). Et slikt team bør ha et formalisert mandat som inkluderer nødvendige fullmakter.

2.7.2 Sambandskatalog

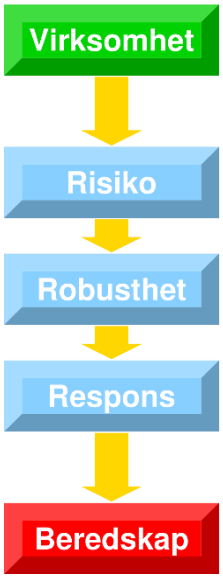
Det skal foreligge en oversikt over kontaktpunkter hos parter det kan være relevant å varsle og/eller søke støtte fra i forbindelse med pågående sikkerhetshendelser. Denne kan ved fordel være koordinert med kontaktlister for kontinuitets- og beredskapsplaner.

2.7.3 Oppfølging

Det bør foreligge retningslinjer for å plukke opp erfaringer fra håndtering av hendelser og benytte disse til å styrke forebygging og senere håndtering av lignende hendelser. Slik oppfølging vil ofte skje utenfor hendelseshåndteringsfunksjonen, og det vil derfor være behov for rutiner for overlevering.

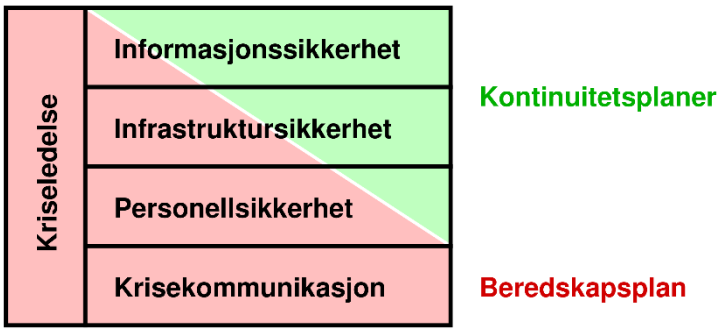
2.8 Kontinuitetsplanlegging

Beredskapsplanen aktiveres når det løpende robusthets- og responsarbeidet ikke er tilstrekkelig til å opprettholde organisasjonens påkrevde tjenestenivå.



Beredskapsplanen spenner over flere fagområder, og ligger utenfor ledelsessystemet for informasjonssikkerhet. Denne planen vil inneholde organisering av kriseledelse og kriterier for hva som defineres som en beredskapssituasjon. I tillegg dekker den typisk egne rutiner for krisekommunikasjon, samt noen områder innenfor personellsikkerhet, infrastruktursikkerhet og

informasjonssikkerhet. Imidlertid vil det innenfor disse tre områdene i ulik grad være behov for system- eller tjenestespesifikke planer for å opprettholde kontinuitet.



Det stilles krav om kontinuitetsplanlegging både i Kunnskapsdepartementets policy for informasjonssikkerhet og personvern og i personvernlovgivingen.

Utvelgelse av hvilke systemer og tjenester som trenger kontinuitetsplaner bør basere seg på en virksomhetskritikalitetsvurdering (BIA, *Business Impact Analysis*). Basert på denne vurderingen prioriteres hvilke systemer og tjenester som først skal reetableres etter en hendelse som gjør at normal drift ikke er mulig. I denne prosessen er det naturlig å ta utgangspunkt i verdioversikten kombinert med en oversikt over tekniske avhengigheter.

Kontinuitetsplaner for de enkelte systemene og tjenestene består av prosedyrer og beskrivelse av nødvendige fasiliteter som muliggjør å gjenopprette driften etter en kritisk hendelse. Kriterier for når kontinuitetsplaner skal settes i verk bør defineres i den overordnede beredskapsplanen.

2.9 Øvelser

2.9.1 Årlig plan for øvelser

Årsplanen for informasjonssikkerhetsarbeidet vil kunne inneholde oversikt over planlagte øvelser som helt eller delvis omfatter fagområdet. Informasjonssikkerhetsansvarlig skal følge opp planen og rapportere status for gjennomføring av planen til ledelsen. Dersom øvelser avdekker mangler ved sikkerhetssituasjonen eller sikkerhetsarbeidet skal dette behandles på samme måte som andre sikkerhetsfunn.

Øvelser spenner fra enkle skrivebordsøvelser og testgjennomføring av utvalgte rutiner til spilløvelser som kan omfatte større deler av virksomheten.

2.9.2 Oppfølging

Det er naturlig at funn fra øvelser inngår i virksomhetens system for avvikshåndtering, inkludert varsling av alvorlige funn til ledelsen.

2.10 Revisjon

2.10.1 Årlig plan for revisjoner

Årsplanen for informasjonssikkerhetsarbeidet vil kunne inneholde oversikt over planlagte sikkerhetsrevisjoner. Informasjonssikkerhetsansvarlig skal følge opp planen og rapportere status for gjennomføring av planen til ledelsen.

To hovedtyper revisjoner er aktuelle:

- Etterlevelsesrevisjon, det vil si å undersøke om vedtatte rutiner og retningslinjer etterleves og er hensiktsmessige.
- Revisjon av hvorvidt eksisterende sikringstiltak er i tråd med relevante anbefalinger om beste praksis, som ISO/IEC 27001: 2022, vedlegg A, eller NSMs grunnprinsipper for IKT-sikkerhet.

Revisjon kan foretas av interne ressurser dersom man har kompetansen tilgjengelig eller av en ekstern aktør. Eksternrevisjon kan utføres av rådgivningstjenesten i eduCSC eller av aktører i det kommersielle markedet. En eventuell tilsynsrevisjon fra for eksempel NOKUT eller Riksrevisjonen vil ikke inngå i en årsplan, men resultatene skal rapporteres og følges opp på lik linje med egeninitierte revisjoner.

2.10.2 Oppfølging

Det er naturlig at funn fra revisjoner inngår i virksomhetens system for avvikshåndtering, inkludert varsling av alvorlige funn til ledelsen.

2.11 Øvrige områder som med fordel kan inngå i ledelsessystemet

2.11.1 Utvikling og anskaffelser av IT-løsninger

For å sikre at informasjonssikkerhet og personvern blir ivaretatt ved utvikling og anskaffelser vil det ha stor verdi å stille tydelige krav tidlig i prosessen. Disse kan formaliseres i standardiserte tekster til bruk i anbudsprosesser eller inngå i rammeverk for egen utvikling av løsninger.

2.11.2 Endringshåndtering (*change management*) og konfigurasjonsstyring

Rutiner for håndtering av oppgradering eller andre endringer av systemer kan bidra til å unngå uforutsette virkninger. Tilsvarende kan systematisk konfigurasjonsstyring både forebygge uventede konsekvenser og bidra til oppdagelse og gjenopprettelse ved eventuelle feil.

2.11.3 Opplæring og holdningsskapende arbeid

Arbeid med sikkerhetskultur kan også formaliseres som en del av ledelsessystemet. Digitaliseringsdirektoratet har publisert veiledere i kompetanse- og kulturutvikling innen digital sikkerhet og for kartlegging av digital sikkerhetskultur: https://www.digdir.no/informasjonssikkerhet/veileder-i-kompetanse-og-kulturutvikling-innen-digital-sikkerhet/2141

2.11.4 Innebygd personvern

I personvernlovgivingen stilles det krav om *innebygd personvern*. Dette inkluderer også krav om at tiltak for informasjonssikkerheten skal være innebygd i IT-løsningene. Kravet om innebygd informasjonssikkerhet gjelder både ved egenutvikling av IT-løsninger og ved anskaffelser av IT-løsninger. Virksomheten må derfor stille krav til at informasjonssikkerheten er ivaretatt ved utvikling eller anskaffelser.

Krav om innebygd informasjonssikkerhet kan for eksempel omfatte følgende:

- Kryptering ved lagring eller dataoverføring.
- Rollebasert tilgangsstyring.
- Sikkerhetskopiering.
- «Min side»-funksjonalitet.

- Tidsbegrenset lagring.
- Logging av tilganger eller forsøk på tilganger.
- Pseudonymisering.

Virksomheten bør rådføre seg med sin personvernrådgiver ved egenutvikling eller anskaffelser av IT-løsninger for å sikre innebygd informasjonssikkerhet.

Del 3 – kontrollerende dokumenter

Hovedformålet med kontrollerende del er å sikre at ledelsen får innsikt i sikkerhetsarbeidet og det nødvendige grunnlaget for å styre det videre arbeidet i den retningen de ønsker. Et sentralt moment i ISO/IEC 27001:2022 er prinsippet om *kontinuerlig forbedring*, men den viktigste arenaen for ledelsens involvering i arbeidet er den årlige *ledelsens gjennomgang* (LG). Her vil det typisk avgjøres om rammeverket skal justeres eller utvides, og målsetninger for kommende års arbeid settes. Når på året LG gjennomføres er ikke avgjørende, men å sette et noenlunde fast tidspunkt i årshjulet vil gjøre det lettere å sammenligne erfaringer mellom ulike år, og å koordinere med årsbudsjetteringen.

3.1 Årsrapport

Til LG sammenstiller informasjonssikkerhetsansvarlig statusrapporter fra hvert av hovedområdene i gjennomførende del. Disse rapportene behøver ikke følge en felles mal, men tilpasses fagområdets egenart. Områder med mindre omfattende aktivitet kan slås sammen, og ulike rapporter kan ha forskjellig forfatter; for eksempel kan rapporten for hendelseshåndteringsarbeidet utarbeides av IRT-leder.

Rapportene bør inneholde informasjon om aktivitet, ressursbruk, utviklingen i forhold til tidligere år og eventuelle nye trender. Spesielt bør det vektlegges hvorvidt årsplanen ble etterlevd, og årsakene til eventuell manglende etterlevelse. Dersom den ansvarlige for fagområdet behøver avklaringer fra ledelsen eller mener at området ikke har de riktige rammene, verktøyene eller ressursene må dette nevnes eksplisitt.

Rapporten om avvikshåndtering står i en særstilling, og kan med fordel presenteres først. Alvorlige avvik bør nevnes individuelt i kortfattet form, mens øvrige avvik behandles statistisk. Viktige momenter er hvor lenge avvik blir stående åpne før de lukkes, og om antallet åpne avvik har en uheldig utvikling. Her må tallene ses i sammenheng med øvrig aktivitet, siden for eksempel flere risikovurderinger eller innføring av sårbarhetsskanning vil øke antall avdekkede avvik uten noen underliggende utvikling som det må tas hensyn til. Gjentakende avvik innenfor et område er også interessant fordi det kan tenkes at praksisen eller rutinen på området bør endres. Eventuelle åpne alvorlige avvik vil kunne kreve ledelsens involvering å få løst, men LG er ikke den rette anledningen til å behandle enkeltsaker.

3.2 Forslag til endringer i rammeverk

Endringer i rammeverket vil i hovedsak være av tre typer:

- Justeringer av eksisterende sikkerhetsmål, sikkerhetsstrategi og retningslinjer
- Å innlemme eksisterende aktivitet i ledelsessystemet, eventuelt med justeringer
- Opprettelse av nye aktiviteter på området

Informasjonssikkerhetsleder kan selv utforme slike forslag, eller videreformidle forslag fra andre aktører. Hvilket detaljnivå vedtak skal gjøres på er opp til ledelsens tid, interesse og fagkompetanse på området.

Større endringer i ressursbruk vil også inngå i denne delen, og vil kunne ha betydning for budsjettprosessen.

3.3 Forslag til årsplan

Hvert aktivitetsområde i gjennomførende del vil kunne ha sin egen årsplan, men siden sikkerhetsarbeid i stor grad dreier seg om å håndtere det uforutsigbare vil ikke slike planer være dekkende for arbeidet i sin helhet. Imidlertid synliggjør ledelsen her forventet aktivitetsnivå, og kan også beskrive årsmålsetninger på et mer abstrakt nivå.

Typisk vil forslag til årsplaner legges fram av informasjonssikkerhetsansvarlig, eventuelt med opsjoner for ulike ambisjonsnivåer.

3.4 Referat fra gjennomgangen

Både materialet som presenteres for ledelsen og alle vedtak som gjøres må arkiveres på en måte som gjør det enkelt for informasjonssikkehetsansvarlig å følge opp målsetninger og å benytte materialet ved forberedelse til neste LG.

3.5 Andre kontrollerende funksjoner

Ut over LG vil arbeidet med informasjonssikkerhet også ta inn over seg korrigerende signaler fra andre kilder.

- Oppfølging gjennom Units styringsmodell for informasjonssikkerhetsarbeid og personvern
- Ekstern eller intern revisjon av arbeidet med informasjonssikkerhet og personvern
- Eventuell sertifisering etter ISO/IEC 27001:2022