*(****Kommentarer og noen råd er skrevet i gult innledningsvis og underveis i dokumentet.***

*Dette eksempelet er en* ***utdypning og videre konkretisering*** *av retningslinjen «Roller og ansvar». Eksempelet gjelder internkontrollområdet informasjonssikkerhet. Dokumentet bør etableres som en utdypende veiledning dersom det anses nødvendig for å sikre tilstrekkelig forståelse og etterlevelse av internkontrollaktivitetene og ansvaret på informasjonssikkerhets­området.* ***De som gjenbruker sentrale deler av eksempelet, er selv ansvarlig for kvalitetssikring av innholdet og tilpasning til egen virksomhet.****)*

**Innhold**

[1. Innledning 2](#_Toc90502680)

[1.1 Målgruppe 2](#_Toc90502681)

[1.2 Formål 2](#_Toc90502682)

[1.3 Relaterte policyer og retningslinjer 2](#_Toc90502683)

[1.4 Forklaringsmodell internkontroll informasjonssikkerhet 2](#_Toc90502684)

[2. Ledelsens styring og oppfølging 2](#_Toc90502685)

[2.1 Virksomhetsledelsens gjennomgang 2](#_Toc90502686)

[2.2 Delegere og følge opp gjennom linjen 3](#_Toc90502687)

[2.3 Sikre finansielle rammer 3](#_Toc90502688)

[2.4 Kommunisere viktighet 3](#_Toc90502689)

[2.5 Løfte og håndtere problemstillinger gjennom linjen 4](#_Toc90502690)

[2.6 Beredskap og krisehåndtering 4](#_Toc90502691)

[3. Vurdering av risiko 4](#_Toc90502692)

[3.1 Ha oversikt og prioritere 4](#_Toc90502693)

[3.2 Planlegge risikovurdering 5](#_Toc90502694)

[3.3 Gjennomføre risikovurdering 6](#_Toc90502695)

[3.4 Vurdere risiko etter hendelser 6](#_Toc90502696)

[3.5 Vurderer risiko ved anskaffelser og utvikling 6](#_Toc90502697)

[4. Håndtering av risiko 6](#_Toc90502698)

[4.1 Foreslå håndtering av risikoer 6](#_Toc90502699)

[4.2 Godkjenne forslag til risikohåndtering 7](#_Toc90502700)

[4.3 Iverksette godkjente tiltak 7](#_Toc90502701)

[4.4 Utforme og etablere sikkerhetstiltak 7](#_Toc90502702)

[4.5 Oppdatere fellessikring og tilleggssikring 8](#_Toc90502703)

[5. Overvåking og hendelseshåndtering 8](#_Toc90502704)

[5.1 Overvåke i henhold til avtale 8](#_Toc90502705)

[5.2 Rapportere hendelser, avvik og informasjonssikkerhetsbrudd 9](#_Toc90502706)

[5.3 Følge opp hendelser, avvik og informasjonssikkerhetsbrudd 9](#_Toc90502707)

[6. Måling, evaluering og revisjon 9](#_Toc90502708)

[6.1 Vurdere status på eget ansvarsområde 9](#_Toc90502709)

[6.2 Måle tilstanden på definerte indikatorer 10](#_Toc90502710)

[6.3 Gjennomføre evalueringer 10](#_Toc90502711)

[6.4 Gjennomføre internrevisjon 10](#_Toc90502712)

[7. Kompetanse- og kulturutvikling 11](#_Toc90502713)

[7.1 Identifisere og følge opp behov for kompetanse- og kulturutvikling 11](#_Toc90502714)

[7.2 Følge opp lokale sikkerhetskoordinatorer 11](#_Toc90502715)

[7.3 Øvelser 11](#_Toc90502716)

[8. Kommunikasjon 11](#_Toc90502717)

[8.1 Formidle nye føringer 11](#_Toc90502718)

[8.2 Dokumentere gjennomførte styringsaktiviteter 12](#_Toc90502719)

[8.3 Dokumentere etterlevelse av sikkerhetstiltak 12](#_Toc90502720)

[8.4 Statusrapporter som grunnlag for risikovurderinger 12](#_Toc90502721)

[8.5 Saksnotat til virksomhetsledelsens gjennomgang 12](#_Toc90502722)

[8.6 Kommunikasjon mellom aktiviteter og aktører 12](#_Toc90502723)

[8.7 Dialog med styrende organ 12](#_Toc90502724)

[8.8 Ekstern kommunikasjon 12](#_Toc90502725)

# Innledning

## Målgruppe

Målgruppen for dette dokumentet er ledere på alle nivå. Dokumentet er en veiledning og en del av virksomhetens styrende dokumenter.

## Formål

Formålet er å sikre tilstrekkelig internkontroll (styring og kontroll) på informasjonssikkerhets­området. Dokumentet er en utdypning på informasjonssikkerhets­området av retningslinjen *Roller og ansvar i internkontroll- og sikkerhetsarbeidet*.

Dokumentet er strukturert etter styringsaktiviteter og beskriver hvilke delaktiviteter som skal gjennomføres, hvem som har ansvaret for de ulike oppgavene og krav til gjennomføringen.

## Relaterte policyer og retningslinjer

Dokumentet må sees i sammenheng med

* Policy for informasjonssikkerhet
* Retningslinjene
	+ Roller og ansvar
	+ Forstå, vurdere og håndtere risiko
	+ Vurdere behov for risikovurderinger

## Forklaringsmodell internkontroll informasjonssikkerhet

Internkontrollarbeidet er basert på forklaringsmodellen under. Dette dokumentet er strukturert etter hovedaktivitetene i forklaringsmodellen.



# Ledelsens styring og oppfølging

## Virksomhetsledelsens gjennomgang

Virksomhetsledelsen skal minimum årlig gå gjennom status for internkontroll (styring og kontroll) på informasjonssikkerhets­området. Hele toppledergruppen skal i størst mulig grad delta. Omfang og innretning skal være tilpasset risiko og vesentlighet. Gjennomgangen skal være forberedt av fagansvarlig informasjonssikkerhet i samsvar med føringer fra Direktør og tidligere gjennomganger.

Direktør skal på bakgrunn av gjennomgangen gi eventuelle tilleggsføringer for virksomhetens internkontrollarbeid innen informasjonssikkerhet.

Ved behov skal Direktør sørge for etablering eller endring føringene. Fagansvarlig informasjonssikkerhet skal normalt være saksbehandler og resten av organisasjonen skal involveres på hensiktsmessig måte.

Ved behov for mer informasjon om status, kan Direktør beslutte at virksomheten skal måle tilstanden på definerte indikatorer over tid, eller få gjennomført evalueringer eller internrevisjon, jf. pkt. 6.2, 6.3 og 6.4.

## Delegere og følge opp gjennom linjen

Ledere på alle nivå skal jevnlig vurdere hva som er hensiktsmessig oppdeling og gruppering av underliggende områder, arbeidsoppgaver og IKT-system, og på hvilken måte det operative ansvaret som risikoeier, systemeier og felles tiltaksleverandør eventuelt skal delegeres. Tiltak skal være tilpasset risiko og vesentlighet.

Ledere som er mål- og resultatansvarlige for et område, vil ofte automatisk få delegert rollen som risikoeiere for området. Avvik fra dette bør dokumenteres spesielt.

Systemeiere fellessystem og felles tiltaksleverandører, kan helt eller delvis få tildelt eller delegert sitt ansvar gjennom retningslinjer eller forhold som ligger utenfor informasjons­sikkerhet. Oppfølging av at ansvaret etterleves, skal uansett skje gjennom linjen.

Ledere på alle nivå skal jevnlig vurdere om noen styringsaktiviteter bør gjennomføres som fellesaktiviteter på et høyere organisatorisk nivå enn delegeringen tilsier. Målet er å sikre en kostnadseffektiv gjennomføring av internkontrollarbeidet.

All oppfølging av ansvar og oppgaver skal skje som en del av den ordinære linjestyringen, årsplanleggingen og årsoppfølgingen.

Det skal fremgå av dokumentasjonen i linjestyringen at delegering og oppfølging også har omfattet aktivitetene innen internkontroll på informasjonssikkerhetsområdet.

## Sikre finansielle rammer

Ledere på alle nivå skal sørge for at økonomiske erfaringer og behov rundt styringsaktiviteter og sikkerhetstiltak er tema når budsjettrammer vurderes og diskuteres i virksomheten.

Å sikre nødvendige finansielle rammer skal primært skje i de ordinære budsjettprosessene. Budsjettene må samtidig settes opp slik at virksomheten har handlingsrom til å iverksette nødvendige tiltak som blir identifisert gjennom året.

## Kommunisere viktighet

Ledere på alle nivå skal kommunisere viktigheten av både informasjonssikkerhet, de iverksatte sikkerhetstiltakene og de systematiske aktivitetene i internkontrollarbeidet.

Ledelsens holdning kommer til uttrykk gjennom det ledelsen sier og gjør. Kommunikasjonen skal derfor skje både muntlig, skriftlig og gjennom synlig handling.

## Løfte og håndtere problemstillinger gjennom linjen

Dersom problemstillinger i internkontrollarbeidet ikke kan løses på det organisatoriske nivå de oppstår, skal de løftes gjennom linjen og håndteres på et høyere ledernivå.

De skal løftes gjennom linjen til man når et ledernivå som har økonomisk handlingsrom eller myndighet til å finne budsjettdekning, akseptere aktuelle risikoer eller ta andre nødvendige beslutninger.

## Beredskap og krisehåndtering

Ledere på alle nivå skal ha oversikt over behovet for beredskaps- og kriseplaner for sitt ansvarsområde, og sørge for etablering av slike der det er nødvendig. De skal kjenne beredskaps- og kriseplaner der de har en rolle, systematisk øve på relevante situasjoner og være i stand til å ta sin rolle i beredskaps- og krisesituasjoner.

# Vurdering av risiko

Vurdering av risiko skal organiseres og gjennomføres av risikoeiere for et ansvarsområde og av systemeiere for fellessystem. Risikoeierne er systemeiere for egne IKT-system, og disse er en del av deres ansvarsområde.

Det presiseres at risikoeiere som bruker fellessystem, også er risikoeiere for egen informasjonsbehandling i fellessystemene. De skal derfor i tilstrekkelig grad og på hensiktsmessig måte involveres i risikovurderingsarbeid og andre internkontrollaktiviteter som utføres på fellessystemene. Både systemeiere fellessystem og risikoeierne selv har ansvaret for å sikre dette.

## Ha oversikt og prioritere

Foranalyse

Risikoeiere skal på et overordnet nivå identifisere oppgaver og tjenester de har ansvar for, informasjonsbehandlingen i disse, regelverk som må følges og hvilke IKT-system de benytter. De bør også avklare tilgrensende behov knyttet til personvern, og følge opp dette i henhold til egne rutiner.

Risikoeiere skal deretter anslå høyeste konsekvensnivå[[1]](#footnote-1) ved brudd på konfidensialitet, integritet og tilgjengelighet rundt egne arbeidsoppgaver, benyttede IKT-system og spesielle hjelpemidler. Referanserammen skal være oppgavene risikoeierne utfører, informasjonen som behandles og konsekvensnivåene i retningslinjen *Forstå, vurdere og håndtere risiko*.

Systemeiere fellessystem skal som første trinn i sine foranalyser anslå høyeste konsekvens­nivå ved brudd på konfidensialitet, integritet og tilgjengelighet rundt fellessystemene de har ansvar for. De kartlegginger og vurderinger som er gjort av risikoeiere som benytter fellessystemene, jf. foran, er viktig bakgrunnsinformasjon. Referanserammen er den samme.

Både risikoeiere og systemeiere fellessystem skal deretter gjøre en overordnet vurdering av nivået på relevante trusler, farer og sårbarheter og merke seg de som peker seg spesielt ut.

Til slutt kan foranalysene med fordel oppsummeres med noen stikkord om eventuelle områder eller forhold man må være spesielt oppmerksom på i det videre risikoarbeidet.

Analysere eksterne krav

Risikoeiere og systemeiere fellessystem skal ha oversikt over hvilke regelverk og avtaler som gjelder for arbeidsoppgavene og IKT-systemene de har ansvar for og hva kravene i disse medfører i praksis. Oversikten skal benyttes i risikovurderinger og risikohåndtering.

Dersom relevante krav ikke er identifisert og konkretisert på virksomhetsnivå, skal risiko- og systemeierne selv sørge for at kravene blir identifisert, analysert og i tilstrekkelig grad konkretisert.

**Gruppere og dele opp**

For å få fokus på det viktigste, behandle like ting sammen og få målrettet tidsbruk på konkrete risikovurderinger, skal både risikoeiere og systemeiere fellessystem gruppere det som anses enkelt og oversiktlig og dele opp og skille ut det som anses kritisk eller som det er knyttet spesiell usikkerhet til. Det gjelder både arbeidsoppgaver, IKT-system og deler av disse. Resultatet fra foranalysene skal være bakgrunn og støtte.

Vurdere behov for risikovurderinger

Både risikoeiere og systemeiere fellessystem skal deretter systematisk vurdere behovet for oppdaterte eller nye risikovurderinger for de ulike delene av eget ansvarsområde. De skal også prioritere mellom nødvendige risikovurderinger. Vurdering og prioritering skal følge retningslinjen *Vurdere behov for risikovurderinger*.

Oversikt over risikovurderinger

Risikoeiere og systemeiere fellessystem skal ut fra ovennevnte og de risikovurderinger som faktisk gjennomføres, vedlikeholde en oversikt over planlagte og gjennomførte risikovurderinger innen eget ansvarsområdet.

Oppdateringer

Resultatet fra det å få oversikt og prioritere skal revurderes og eventuelt oppdateres minst en gang årlig. Relevante deler av aktiviteten skal alltid gjennomføres og oppdateres før nye oppgaver eller tjenester starter, eller før nye IKT-system anskaffes og tas i bruk.

Støtte

Dersom ikke særskilte grunner tilsier noe annet, skal de veiledninger, maler og verktøy som virksomheten stiller til disposisjon benyttes i arbeidet med å få oversikt og prioritere.

Risikoeiere og systemeiere fellessystem er ansvarlig for gjennomføring og resultat, men de skal få støtte fra virksomhetens felles prosessledere minimum første gang arbeidet gjennomføres.

## Planlegge risikovurdering

Før en risikovurdering starter skal den planlegges. Omfanget av planleggingen skal tilpasses behovet. Planlegging skal skje i samarbeid mellom risikoeier/systemeier fellessystem og den de peker ut som prosessleder for arbeidet. Dette kan være en av virksomhetens felles prosessledere eller andre, avhengig av kompleksiteten i risikovurderingen og tilgjengelige ressurser.

Dersom ikke særskilte grunner tilsier noe annet, skal de veiledninger virksomheten stiller til disposisjon benyttes.

Mandatet for risikovurderingen kan utformes slik at arbeidet skal omfatte både aktiviteten *Gjennomføre risikovurdering,* jf. pkt. 3.4, og oppfølgingsaktiviteten *Foreslå håndtering av risikoer*, jf. pkt. 4.1

## Gjennomføre risikovurdering

Risikoeiere og systemeiere fellessystem skal sørge for at nødvendige risikovurderinger innen eget ansvarsområde blir gjennomført. Et viktig grunnlag er oversikten man utarbeidet under delaktiviteten *Ha oversikt og prioritere*.

Gjennomføring av risikovurderinger skal skje i samsvar med retningslinjen *Forstå, vurdere og håndtere risiko*. Dersom ikke særskilte grunner tilsier noe annet, skal i tillegg de veiledninger og støtteverktøy virksomheten stiller til disposisjon benyttes.

Utpekt prosessleder skal sørge for at risikovurderingene gjennomføres på en måte som er tilpasset objektet for risikovurderingen og de planer som er lagt, jf. pkt. 3.3.

Risikoer som ikke kan aksepteres ut fra retningslinjen *Forstå, vurdere og håndtere risiko* skal gjennomgå aktiviteten *Foreslå håndtering av risikoer*, jf. pkt. 4.1.

## Vurdere risiko etter hendelser

Risikoeier og systemeier fellessystem kan under hendelseshåndtering oppdage alvorlige uønskede hendelser man ikke har vært tilstrekkelig oppmerksom på i tidligere risikovurderinger.

De skal da sørge for at det blir gjennomført en avgrenset behovsvurdering og eventuelt påfølgende risikovurdering og risikohåndtering for denne og relevante tilgrensende hendelser.

Risiko- og systemeierne er ansvarlig for at dette blir gjennomført effektivt og i tide, f.eks. ved egne prosedyrer i egen organisatoriske enhet.

## Vurderer risiko ved anskaffelser og utvikling

Ved anskaffelse eller utvikling av IKT-systemer, skal aktuell systemeier sørge for at behovene og kravene beskrives i behovs- og/eller kravlister. Disse kan utformes i forkant av anskaffelsen eller gradvis i anskaffelses- eller utviklingsprosessen, avhengig av hvilken fremgangsmåte man benytter.

Enkelte overordnede sikkerhetsmessige behov, som at systemet skal ha tilgangsstyring og pålogging, kan identifiseres med samme analytiske tilnærming som ved identifiseringen av funksjonelle behov. Enkelte krav kan også bli avdekket gjennom aktiviteten *Analysere eksterne krav*, jf. pkt.3.1.

For å få en tilstrekkelig identifisering av sikkerhetsbehovene, skal systemeierne også vurdere behovet for, og eventuelt gjennomføre, en eller en serie risikovurderinger, avhengig av om kravene skal utformes i forkant eller underveis i anskaffelses- eller utviklingsprosessen.

Risikoer som i utgangspunktet ikke kan aksepteres som de er, kan ofte presenteres som behov som leverandøren må finne løsning på. Løsningsforslagene vil da være forslag til risikoreduserende tiltak som må vurderes av systemeier. Ved enighet vil disse tiltakene representere krav til IKT-systemet.

# Håndtering av risiko

## Foreslå håndtering av risikoer

For risikoer som ikke kan aksepteres i risikovurderingen, jf. pkt.3.4, skal risikoeier / systemeier fellessystem sørge for at eventuelle tiltak som kan redusere risikoene blir identifisert og vurdert. Arbeidet skal skje i samsvar med retningslinjen *Forstå, vurdere og håndtere risiko*. Arbeidet kan være en del av et større helhetlig oppdrag gitt i mandatet til risikovurderingen.

Dersom ikke særskilte grunner tilsier noe annet, skal de veiledninger og støtteverktøy virksomheten stiller til disposisjon benyttes.

## Godkjenne forslag til risikohåndtering

Dokumentasjonen av risikovurderinger og forslag til håndtering av risikoer er et beslutningsgrunnlag.

Oppdragsgiver, dvs. aktuell risikoeiere eller systemeier fellessystem, skal alltid foreta en selvstendig vurdering av dette beslutningsgrunnlaget. Vurderingen skal skje i samsvar med retningslinjen *Forstå, vurdere og håndtere risiko*. Dersom ikke særskilte grunner tilsier noe annet, skal for øvrig de veiledninger virksomheten stiller til disposisjon benyttes.

En systemeier fellessystem må avstemme sin vurdering med risikoeiere som benytter systemet. Ved uenighet må aktuelle problemstillinger løftes til et høyere beslutningsnivå.

Dersom oppdragsgiver ser behov for at det blir gjort nye vurderinger for at han skal kunne ta en beslutning, må han sørge for at dette blir gjort.

Oppdragsgiver har ansvaret for å få finansiert godkjente forslag. Dersom oppdragsgiver ikke disponerer tilstrekkelige budsjettmidler, må problemstillingen løftes gjennom linjen, jf. pkt. 2.5.

Dersom oppdragsgiver ikke har myndighet til å akseptere restrisikoer for oppgaver han har ansvaret for og som han mener må utføres, må problemstillingen rundt disse risikoene løftes gjennom linjen.

## Iverksette godkjente tiltak

Når forslag til risikohåndtering er godkjent og finansiert, skal oppdragsgiver peke ut en håndteringsansvarlig som skal planlegge og følge opp den samlede gjennomføringen eller etableringen av godkjente tiltak.

Oppdragsgiver kan selv være håndteringsansvarlig der det anses hensiktsmessig. Dersom det er en annen person, skal denne systematisk følges opp av oppdragsgiver.

Håndteringsansvarlig skal utforme en handlingsplan for gjennomføring eller etablering av de godkjente tiltakene. Planen bør utformes i dialog med de som skal gjennomføre aktivitetene. Planleggingen skal følge god praksis for prosjekt- og aktivitetsplanlegging generelt, og ha fokus på tid, kost og forventet effekt av tiltakene.

Planen skal inneholde frister og hva som skal gjøres av hvem. Formalisme og detaljeringsnivå skal tilpasses

* tiltakenes viktighet
* omfang og kompleksitet på det som skal gjøres
* hvem som skal være ansvarlig
* hvordan virksomheten har organisert seg internt

Handlingsplanen skal godkjennes av oppdragsgiver før den iverksettes.

Håndteringsansvarlig skal systematisk følge opp fremdriften. Nødvendig rapportering skal skje til oppdragsgiver i samsvar med de føringer som er gitt.

## Utforme og etablere sikkerhetstiltak

Konkrete tiltak utformes, iverksettes og vedlikeholdes av tiltaksleverandører.

Hvem som er felles tiltaksleverandør for ulike fellesområder i virksomheten, fremgår av retningslinjen *Roller og ansvar***.**

Risikoeier og systemeier fellessystem kan i tillegg selv være tiltaksleverandør for enkelte tiltak knyttet til egne arbeidsoppgaver eller IKT-system. Dette vil ofte være krav, prosedyrer, rutiner, kompetanse- og kulturutvikling o.l.

Tiltaksleverandører skal utforme og implementere tiltak i samsvar med avtaler gjort med ulike håndteringsansvarlige, jf. pkt. 4.3. Dokumentasjon av tiltakene skal skje i henhold til anerkjent god praksis og de krav som er stilt fra risikoeier og systemeier fellessystem.

Tiltakene må testes slik det er avtalt. Det bør i den grad det er nødvendig skje under både utforming, implementering, gjennomføring og i kontinuerlig bruk. Dersom tester under etablering eller senere drift viser at tiltakene ikke fungerer som avtalt, må de justeres. Dette bør inngå i avtalt vedlikehold.

Risikoeier og systemeier fellessystem er ansvarlig for at nødvendig testing, undersøkelser og vedlikehold blir avtalt med både interne og eksterne tiltaksleverandører.

Felles tiltaksleverandører skal systematisk oppdatere en oversikt over etablerte sikkerhetstiltak og deres tiltaksstyrke. Det skal skje i det system som er etablert for formålet.

## Oppdatere fellessikring og tilleggssikring

De tiltak som skal gjennomføres eller implementeres, kan i utgangspunktet etableres som del av virksomhetens felleskring[[2]](#footnote-2), eller som tilleggssikring som risikoeiere og systemeiere kan velge ut fra behov.

Tiltaksleverandørene skal vurdere hva virksomheten samlet er best tjent med. Det skal skje allerede i dialogen med håndteringsansvarlig. Tiltaksleverandørene skal i første omgang vurdere om innplasseringen som fellessikring eller tilleggssikring gir vesentlige forskjeller mht. kostnadseffektiv drift av sikkerhetsarbeidet. De bør også gjøre en enkel vurdering av negative sideeffekter for andre oppgave- og systemeiere dersom tiltaket blir en del av fellessikringen.

Dersom sideeffektene anses små, eller kostnadsvurderingen klart taler for en endring i fellessikringen, skal spørsmålet om en slik endring oversendes til fagansvarlig informasjonssikkerhet.

Dersom fagansvarlig informasjonssikkerhet er enig, skal han initiere og lede en grundigere vurderingsprosess. Det skal da gjennomføres en identifisering av negative sideeffekter for andre arbeidsoppgaver og IKT-systemer, samt estimering av kostnader. I tillegg skal de som blir berørt av sideeffektene få uttale seg.

Endelig beslutning om utvidelse av fellessikringen skal tas av Direktør eller den han utpeker.

# Overvåking og hendelseshåndtering

## Overvåke i henhold til avtale

Overvåking er et sikkerhetstiltak som velges og utformes i risikohåndteringen på linje med øvrige tiltak, jf. pkt.4. Slike tiltak skal inneholde informasjon om hva som skal overvåkes, hvem som er ansvarlig for overvåkingen og hvordan resultatet av overvåkingen skal rapporteres.

For eksterne tiltaks- eller tjenesteleverandører skal kravene om overvåking være nedfelt i en tjenestenivåavtale (SLA).

Det skal ikke etableres overvåkingstiltak av ansatte eller andre personer, dersom tiltakene ikke er utviklet og innført i samsvar med regelverk, avtaler og tilstrekkelig involvering av de det gjelder eller deres representanter.

## Rapportere hendelser, avvik og informasjonssikkerhetsbrudd

Alle ansatte og innleide med tilgang til systemer og informasjon er ansvarlig for å rapportere hendelser, avvik og informasjonssikkerhetsbrudd de oppdager eller mistenker.

Rapporteringen skal skje etter kravene i vårt system for hendelses- og avvikshåndtering, uten unødig opphold etter at hendelsen er oppdaget.

## Følge opp hendelser, avvik og informasjonssikkerhetsbrudd

Systemet for hendelses- og avvikshåndtering er et sikkerhetstiltak som skal ha klare ansvarsforhold og prosedyrer om både håndtering og kommunikasjon.

Det skal til enhver tid være minst en person som er ansvarlig for å følge opp innrapporterte hendelser og rute dem videre til rette vedkommende. Det skal være planlagt for ferieavvikling og annet fravær. Det skal følges opp at innrapporterte hendelser av ulik type håndteres innen gitte frister.

Alle rapporterte hendelser, avvik eller informasjonssikkerhetsbrudd skal følges opp av rette vedkommende uten unødig opphold. Ved behov skal beredskapsplaner eller andre konsekvensreduserende tiltak iverksettes uten ugrunnet opphold.

Det skal alltid vurderes om vi kan lære av erfaringene fra en hendelse. Særlig skal det vurderes om hendelsene og avvikene tilsier justering av risikovurderinger og tilhørende tiltak. Kunnskapen må brukes i det videre arbeidet med vurdering av risiko.

# Måling, evaluering og revisjon

## Vurdere status på eget ansvarsområde

Minst en gang i året skal følgende vurdere status for sine ansvarsområder:

* ledere som delegerer og skal følge opp gjennom linjen
* risikoeiere
* systemeiere fellessystem
* tiltaksleverandører
* ansvarlige for tjenestenivåavtaler eller andre avtaler
* ansvarlige for egne deler av internkontrollaktivitetene, som f.eks. hendelseshåndteringssystemet og internrevisjon

Statusvurderingen skal omfatte vurderinger av om man selv, egne ansatte og leverandører

* følger gjeldende lov- og regelverk
* gjennomfører internkontrollaktivitetene slik man er pålagt
* etablerer og følger opp vedtatte eller avtalte sikkerhetstiltak
* etterlever gjeldende sikkerhetstiltak

I tillegg skal de som har ansvar for tiltak vurdere om tiltakene fungerer som forutsatt.

Alle skal i første omgang vurdere hvor stor tillit de har til at status er slik den skal være. Dersom tilliten er lav, skal nærmere undersøkelser gjennomføres. Dersom tilliten er moderat, skal behovet for nærmere undersøkelser vurderes ut fra hvor viktig saken anses å være, både for virksomheten og egen enhet. Er tilliten høy, er det normalt ingen grunn til ytterligere undersøkelser. Det betinger imidlertid at tillitsnivået bygger på kritisk refleksjon om egen kunnskap.

Den ansvarlige må sørge for at nærmere undersøkelser blir gjort i tilstrekkelig omfang og med tilstrekkelig kvalitet. Dersom undersøkelser avdekker avvik, må disse utbedres slik at ting fungerer og tilliten økes til et tilfredsstillende nivå.

Resultatet av statusvurderingen, sammen med hvilke undersøkelser og oppfølgingstiltak som eventuelt er gjennomført, skal dokumenteres i et kort notat. Rapportering skal skje gjennom linjen. I tillegg skal risikoeiere, som kan ha blitt påvirket av identifiserte svakheter, informeres spesielt om det som er relevant for dem.

## Måle tilstanden på definerte indikatorer

Virksomhetsledelsens kan beslutte at de vil følge tilstanden over tid på enkelte områder, jf. pkt. 2.1.

De skal da peke ut noen ansvarlige som skal utarbeide forslag til systematiske målinger, herunder områder, indikatorer, metoder, frekvens, ansvarlige og rapportering. Beslutning skal tas av virksomhetsledelsen.

Målingene skal gjennomføres av de som blir pekt ut til det gjennom linjebeslutninger.

Resultatene skal sammenstilles av fagansvarlig informasjonssikkerhet og presenteres for virksomhetsledelsen, normalt som del av virksomhetsledelsens gjennomgang.

## Gjennomføre evalueringer

Virksomhetsledelsens kan beslutte at det skal gjennomføres evalueringer, jf. pkt. 2.1. Evalueringer kan omfatte hele eller deler av arbeidet med internkontroll og informasjonssikkerhet i virksomheten.

Ledere på ulikt nivå kan i tillegg beslutte at de skal få gjennomført evalueringer på deler av sine ansvarsområder. Noe av dette kan være lovpålagt, f.eks. krav om «sikkerhetsrevisjoner» e.l.. Slike krav vil normalt dekkes av målrettede evalueringer.

Oppdragsgiver skal peke ut de som skal være ansvarlig for en evaluering. Det skal alltid gjøres en vurdering av behovet for uavhengighet. Ved særskilt behov for uavhengighet eller kompetanse, kan man hente inn eksterne til å gjennomføre evalueringen.

Evalueringsoppdrag skal være spesifisert og avgrenset og gjennomføres på en profesjonell måte. Resultatet skal presenteres for oppdragsgiver. Eventuelle avvik skal følges opp.

## Gjennomføre internrevisjon

Virksomhetsledelsens kan beslutte at det skal gjennomføres internrevisjon, jf. pkt. 2.1. En internrevisjon kan omfatte hele eller deler av arbeidet med internkontroll og informasjonssikkerhet i virksomheten.

Formålet med internrevisjon er å få en formell uavhengig vurdering av om vi følger eksterne og interne krav til arbeidet med internkontroll og informasjonssikkerhet, og om kravene er implementert og vedlikeholdt på en formåls- og kostnadseffektiv måte.

Arbeidet skal gjennomføres etter anerkjente revisjonsstandarder. Arbeidet kan utføres av interne eller eksterne, men reell uavhengighet skal sikres.

Resultatet av en internrevisjon skal presenteres for virksomhetsledelsen. Avvik skal følges opp på en systematisk måte.

# Kompetanse- og kulturutvikling

## Identifisere og følge opp behov for kompetanse- og kulturutvikling

Identifisering av behov for kompetanse- og kulturutvikling skal gjøres løpende som en del av internkontrollarbeidet i virksomheten. Dette skal gjøres av ledere på alle nivå og for alle ansvarsområder.

Behovene kan identifiseres gjennom ulike delaktiviteter, for eksempel

* medarbeidersamtaler
* risikovurderinger
* oppfølging av hendelser, avvik og informasjonssikkerhetsbrudd
* vurdering av status på eget ansvarsområde
* revisjoner og evalueringer
* virksomhetsledelsens gjennomgang

Når det er identifisert et behov skal det gjennomføres hensiktsmessige tiltak. Tiltakene skal

* være tilpasset riktig målgruppe
* ta i bruk hensiktsmessig(e) virkemidler
* sees i sammenheng med andre opplæringstiltak i virksomheten
* være tilrettelagt slik at man kan måle effekten av tiltaket.

## Følge opp lokale sikkerhetskoordinatorer

Fagansvarlig informasjonssikkerhet og virksomhetens lokale sikkerhetskoordinatorer skal møtes jevnlig for å utveksle erfaringer og lære av hverandre.

Aktuelle temaer for samlingene vil være

* sikkerhetskoordinatorenes egen kompetanseheving innen informasjonssikkerhet og internkontroll
* kompetanse- og kulturutfordringer rundt om i virksomheten og innspill og råd til sentralstyrte tiltak på området
* innspill og råd til virksomhetsledelsens gjennomgang
* innspill og råd rundt fellessikring i virksomheten

## Øvelser

Virksomhetsledelsen er ansvarlig for at det minst en gang i året gjennomføres en øvelse på informasjonssikkerhetsområdet. Fagansvarlig informasjonssikkerhet skal være sentral i gjennomføringen. Øvelsene skal evalueres, slik at man fanger opp behov for kompetanseheving eller andre forbedringsbehov.

# Kommunikasjon

## Formidle nye føringer

Nye eller oppdaterte føringer skal formidles raskt og effektivt til de som har eller kan få bruk for dem. Ansvaret ligger hos de som godkjenner føringene. Dokumentasjon og formidlingskanal skal være i samsvar med våre felles krav til dokumentasjon av internkontroll.

De ansvarlige skal alltid vurdere om det i tillegg er behov for egne informasjonsmøter, opplæringstiltak o.l. Formålet er å forsikre seg om at informasjonen er tilgjengelig for mottakerne når de har behov for den, at den er forstått, samt at mottakeren har holdninger og tilstrekkelig kompetanse til å etterleve føringene. Ved behov skal den ansvarlige sørge for at hensiktsmessige tiltak blir gjennomført.

## Dokumentere gjennomførte styringsaktiviteter

Gjennomføring av styringsaktiviteter beskrevet i denne dokumentet skal som hovedregel dokumenteres skriftlig. Et kort notat vil ofte være nok. Arkivering og journalføring skal skje i samsvar med våre felles krav til dokumentasjon av internkontroll.

## Dokumentere etterlevelse av sikkerhetstiltak

Dersom sikkerhetstiltak, prosedyrer eller rutiner stiller krav om det, skal etterlevelsen av dem dokumenteres skriftlig. Slike krav skal være basert på risiko og behov. Eventuelle dokumentasjonskrav på etterlevelse skal være en del av beskrivelsen av tiltaket.

Dokumentasjonskrav skal legges opp på en måte som gjør at de ikke oppleves som unødvendige eller vesentlig hemmende for annet viktig arbeid.

## Statusrapporter som grunnlag for risikovurderinger

Fagansvarlig informasjonssikkerhet skal i januar hvert år lage en rapport over status og trender på informasjonssikkerhetsområdet både internt i virksomheten og i sammenlignbare virksomheter eksternt. Rapporten skal være bakgrunnskunnskap for de som skal vurdere risiko rundt om i virksomheten. Rapporten må være tilpasset det formålet.

## Saksnotat til virksomhetsledelsens gjennomgang

Fagansvarlig informasjonssikkerhet skal senest to uker før virksomhetsledelsens gjennomgang produsere et saksnotat til gjennomgangen. Det skal også utarbeides og legges ved en tilpasset rapport om status på relevante områder innen informasjonssikkerhet. Notatet og rapporten skal være tilpasset de føringer virksomhetsledelsen har gitt fra tidligere gjennomganger.

## Kommunikasjon mellom aktiviteter og aktører

Alle aktiviteter i denne dokumentet forutsetter en rask og effektiv kommunikasjon med andre aktiviteter og mellom ulike aktører. Det er et ansvar for alle ansatte å bidra til at riktig informasjon kommer frem til riktig person til riktig tid. Ivaretagelse av lovpålagt taushetsplikt ligger i begrepet *riktig informasjon til riktig pe*rson.

## Dialog med styrende organ

Status på arbeidet med styring av informasjonssikkerhet skal rapporteres til styrende departement i etterkant av virksomhetsledelsens gjennomgang, i årsrapporten og i den løpende styringsdialogen etter behov.

## Ekstern kommunikasjon

Eventuell kommunikasjon med personer utenfor vår virksomhet om risikoer, tiltak, internkontroll, informasjonssikkerhet, mv., skal skje i samsvar med vår policy og retningslinjer for ekstern kommunikasjon. Det gjelder både innhold og hvem som uttaler seg om hva.

Lovpålagt taushetsplikt og offentleglovas bestemmelser om unntatt offentlighet og meroffentlighet skal ligge til grunn for all kommunikasjon.

1. «Høyeste konsekvensnivå» er det høyeste nivået på konsekvenser på området som man med en viss grad av sannsynlighet må regne med kan inntreffe. Urealistiske utfall holdes derfor utenfor. [↑](#footnote-ref-1)
2. Fellessikring er et sett av sikkerhetstiltak som er etablert for å gi et felles grunnleggende sikkerhetsnivå for sentrale områder av virksomheten [↑](#footnote-ref-2)