Voss herad

# Retningslinje for gjennomføring av risiko- og sårbarheitsanalyse (ROS) innan personvern og informasjonssikkerheit

## 1 Mål

Risikostyring er eit viktig verktøy i mål- og resultatstyringa i Voss herad. For å kartlegge risiko knytt til eit bestemt system, prosess, teneste eller ei behandling av personopplysningar skal me gjennomføre ei ROS. Målsettinga er å få oversyn over risikobiletet, og kunne prioritera ressursar effektivt, for å setta i gang naudsynte tiltak slik at me kan redusera eventuelle risikoar.

## 2 Retningslinja gjeld for

Alle tilsette i Voss herad

## 3 Ansvar

Retningslinja er vedteken av Rådmann
Eigar av retningslinja er Stabssjef for Innbyggjarservice.
Rådgjevar for personvern er ansvarleg for at retningslinja er oppdatert med omsyn til gjeldande regelverk.

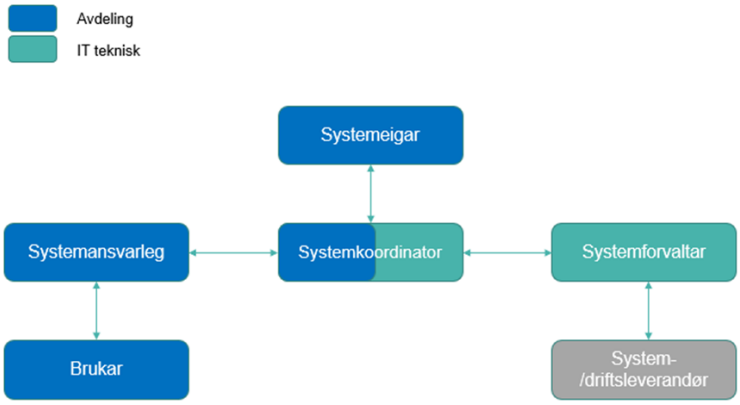
## 4 Retningslinja

### Når må me gjennomføre ein ROS?

ROS av eit system, ein prosess, teneste eller behandling av personopplysningar skal gjennomførast før dei vert tekne i bruk. Om ein ROS vert gjort for eit prosjekt eller ei anskaffing, skal det inngå som ein del av prosjekt- eller anskaffingsprosessen. Den første ROS vil danne grunnlaget for vurderingar som vert gjort på eit seinare tidspunkt.
Om Voss herad vurdere å sette ut ei eller fleire oppgåver til eksterne aktørar, skal det fyst gjennomførast ein ROS. Omfanget av vurderinga kan verte tilpassa utkontrakteringens betydning og omfang. Utkontraktering kan ikkje gjennomførast om det inneber ein høg risiko for personvern og informasjonssikkerhet.

## Roller og ansvar

For at risikostyringa i Voss herad skal fungere godt krev det at rollene som er definert i IKT forvaltningsmodellen følg opp ansvarsområda dei er tildelte, og at dei samhandlar godt med kvarandre.
Forvaltningsmodellen og rollene kan du lese meir om i dokumentet «Handbok for innføring av IKT forvaltningsmodell i Voss herad».




Under følg ei kort skildring av dei mest sentrale rollene i denne samanheng.

1. Systemeigar skal sikre at det vert gjennomført risikovurderingar av systemet i samsvar med Voss herad sine prosedyrar, og at risikovurderingar vert oppdatert jamleg og ved vesentlege endringar. Systemeigar skal sikre at det vert gjennomført personkonsekvensvurderingar av systemet, og løfte vesentlege og uakseptable risikoar til systemkoordinator/ sikkerheitsforum om tilstrekkelege risikoreduserande tiltak ikkje kan settast i verk for å redusere risiko til eit akseptabelt nivå.

2. Systemansvarleg skal gjennomføre risikovurderingar av systemet i samsvar med Voss herad sine prosedyrar, og syte for at risikovurderingar vert oppdatert jamleg og ved vesentlege endringar. Systemansvarleg skal bidra til at det vert gjennomført personkonsekvensvurderingar av systemet ved behov, og løfte risikoar til systemeigar

3. Systemkoordinator skal gje råd ved gjennomføring av risikovurderingar av IKT system og løysingar, spesielt ved anskaffing av nye. Systemkoordinator skal bistå med rådgjeving i eiga avdeling der risikoreduserande tiltak ikkje kan settast i verk for å redusere risiko til eit akseptabelt nivå.

4. Systemforvaltar skal bistå ved gjennomføring av risikovurderingar av systemet, og bidra til at det vert gjennomført personkonsekvensvurderingar av systemet ved behov. Systemforvaltar skal løfte risikoar til systemkoordinator

## Kva skal ei ROS innehalde?

For å gjennomføre ei god ROS er det naudsynt å definere omfanget tydeleg. Skildringa skal minimum innehalde informasjon om

- Kva system som er vurdert, og eventuelt andre system det har eit grensesnitt mot
- Kva system(a) vert nytta til
- Kven som er brukarar og tenestemottakar
- Kva data/ informasjon som skal beskyttast og som må inngå i vurderinga
- Eventuelle samarbeidspartar/leverandørar som kan påverke risikobiletet

## Kven skal involverast i ei ROS?

Det er viktig å involvere personar med rett kompetanse for å få fram alle naudsynte risikoar. Det betyr at alle som har ei rolle i forvaltningsmodellen som er knytt til det aktuelle systemet, skal delta. I tillegg kan ein vurdere å hente inn spesialkompetanse på aktuelle områder etter behov. Avhengig av kompleksitet i systemet og driftsmodell bør ein vurdere å ta med leverandørar på delar av ROS analysen, då desse ofte kan seie noko om risikoreduserande tiltak på det tekniske området.

## Korleis vurdere sannsyn og konsekvens for hendingar i ROS?

Risikoen for ei hending vert berekna ut i frå ein kombinasjon av sannsyn og konsekvens. For å systematisere og strukturere dei ulike hendingane i ein ROS skal me nytta eit ferdig utarbeida verktøy. Dette verktøyet vil hjelpe til med å få ei god oversikt på definerte risikoområde og moglege hendingar, samstundes som ein kan knytte desse opp mot sannsyn og konsekvens. Dei hendingane som krev at det vert sett i verk tiltak vil automatisk kunne identifiserast slik at risikobiletet vert synleg.

Voss herad vil ikkje akseptere ein høg risiko for hendingar knytt til personvern og informasjonssikkerheit. Det vil seie at om det inneber ein høg risiko å ta i bruk eit nytt system, prosess, teneste eller behandling av personopplysningar skal det settast i verk risikoreduserande tiltak som gjer at risikoen vert akseptabel før oppstart. Om systemeigar vel å starte opp med høg risiko utan å ha vurdert risikoreduserande tiltak, skal dette meldast som eit avvik.

Om risikoen for ei hending er middels skal det vurderast kva slags risikoreduserande tiltak som kan settast i verk, og det bør gjerast ei kost-nytte vurdering av om det er hensiktsmessig å innføre tiltak. Det betyr at om det har ein lav kostnad og krev lite ressursbruk bør tiltak settast i verk. Om det har ein høg kostnad og krev mykje ressursar vil det normalt sett ikkje vere tilrådeleg å sette inn tiltak. Risiko skal vurderast kontinuerleg, og om den endrar seg til høg skal det settast inn risikoreduserande tiltak omgåande. Om risikoen er låg er det ikkje naudsynt å sette inn risikoreduserande tiltak.

## Korleis gjennomføre ein ROS?

Ei mykje brukt metode for å gjennomføre ROS, er å samle personar med naudsynt kompetanse og bakgrunn til eitt eller fleire arbeidsmøte for å diskutere aktuelle risikoar, sannsyn for at dei skjer,

moglege konsekvensar, og om risikoen er akseptabel eller om det er naudsynt å sette i verk risikoreduserande tiltak, og i så fall kva slags tiltak.

Fokus i risikovurderinga er på risiko for brot på Voss herad sine krav til konfidensialitet, integritet og tilgjengelegheit. I tillegg er det viktig å vere merksam på andre konsekvensar hendingar kan få, eksempelvis knytt til heradet sitt omdøme, tenesteleveransar og økonomiske konsekvensar. Tenesta / løysninga si robustheit bør også vurderast.
Grundig planlegging legg til rette for ein vellykka ROS, og god risikostyring. Møteinnkallingar må sendast ut i god tid for å legge til rette for deltaking frå nøkkelressursar. Det er også fleire ting som må avklarast i denne fasa, som til dømes:

- Omfanget av risikovurderinga
- Tidsplan for gjennomføring.
- Kven som bør delta i gjennomføringa
- Fordeling av roller og ansvar:
  - Kven er systemeigar?
  - Kva systemeigarar og systemkoordinatorar har ei rolle i ROS?
  - Kven er driftsansvarleg, evt. system som er omfatta, og kven som er kontaktpersonen? til desse systema?
  - Kven skal nytte løysinga?
  - Er det behov for å involvere juridisk kompetanse?
  - Kven er ansvarlege for risikoreduserande tiltak?
  - Kven har ansvaret for den praktiske gjennomføringa av ROS?
  - Kven skal dokumentere vurderingar som vert tekne?
- Er relevant dokumentasjon tilgjengeleg?
- Kvar og korleis vert data lagra/ behandla?
- Finst det tidlegare utførte ROS som er relevant for analysen?

Det bør gjennomførast kortfatta planleggingsmøte før ein gjennomfører ROS. Hensikta med planleggingsmøtet er å førebu ROS, og gjere naudsynte praktiske avklaringar, jfr. punkta som er nemnde over. Det bør normalt settast av ein time til gjennomføring av formøtet. I invitasjon til formøtet kan det med fordel leggast inn lenker til Voss herad sine verktøy, rutinar og retningslinjer som er relatert til personvern og informasjonssikkerheit.

## Arbeidsmøte

Vanlegvis vil det være behov for å gjennomføre minst to arbeidsmøte, som begge går over eit par timar. Dette vil sjølvsagt vere avhengig av kompleksitet og omfang på løysinga. Arbeidsmøte kan med fordel også delast inn i ein meir praktisk del (funksjonell) og i ein teknisk del. På den måten kan ein effektivisere gjennomføringa. På den andre sida vil felles arbeidsmøte kunne føre til tverrfaglege diskusjonar og kompetansedeling.

Representantar for linja med god kjennskap til prosessar som er omfatta av risikovurderinga vil normalt måtte delta i heile risikovurderinga, medan det ofte vil være tilstrekkeleg at representantar med teknisk kompetanse deltek i diskusjon av risiko knytt til hendingar av meir teknisk karakter.

Der det er hensiktsmessig kan representantar for leverandørar/ samarbeidspartnarar som kan bidra til å belyse risikoar og sette i verk risikoreduserande tiltak involverast. Leverandøren bør ikkje delta i vekting av risiko, men kan bidra med innspel til kva slags risikoreduserande tiltak som kan settast i verk , og vere tilgjengeleg for avklaringar undervegs.

I forkant av arbeidsmøtet bør alle deltakarar få tilsendt ei lenke til Excel malen som skal nyttast til å dokumentere ROS i arbeidsmøtet, slik at dei kan legge inn aktuelle hendingar og skildringar av årsaka til dei i forkant av møtet.

I arbeidsmøta bør fokus vere på å:

- Identifisere aktuelle hendingar og kva som er årsaka til at dei kan skje. Dess meir konkret hendinga kan skildrast, dess lettare er det å vurdere risiko og identifisere aktuelle risikoreduserande tiltak.

- Kome med argument for sannsyn, og vurdere om det er etablert tiltak som kan redusere sannsynet for hendinga, om det er kjende sårbarheiter som påverkar sannsynet for hendinga, om det har skjedd før, mm. Basert på analysen her må ein fastsette ein talverdi som skal fyllast ut i kolonna for sannsyn.

- Kome med argument for konsekvens, og vurdere om det er etablert tiltak som bidreg til å redusere konsekvensen for den aktuelle hendinga. Basert på analysen må ein fastsette ein talverdi som skal fyllast inn i kolonna for konsekvens

- Vurder kva tiltak som skal eller bør settast i verk for å redusere risiko for utvalde hendingar. Risikoen kan verta redusert med å setta inn tiltak som reduserer sannsyn for at hendinga skjer og/eller konsekvensen om den skjer. Alle risikoreduserande tiltak skal ha ein ansvarleg og frist for gjennomføring.

Det er viktig å vere så konkret som mogleg i skildring av hendingar og tilhøyrande risiko for at det skal være mogleg å identifisere og innføre effektive risikoreduserande tiltak. Det er viktig å skildre vurderingar som vert gjort so godt som mogleg slik at dei kan gje eit oversyn på kva som er gjort i etterkant.

Det kan vere hensiktsmessig å nytte ei sjekkliste over tema som må risikovurderast i arbeidsmøta. For å unngå at sjekklista fører til at andre tema som kan innebere ein risiko ikkje vert vurdert, bør prosessen starta med ei idémyldring. Sjekklista kan nyttast i etterkant for å kontrollere at det er tatt høgde for alle dei sentrale elementa i analysen. Excel malen som nyttast i ROS møte inneheld ei arkfane med tema for risikovurdering.

Det er systemeigar sitt ansvar å syte for at det vert innført tilstrekkelege risikoreduserande tiltak for uakseptable risikoar før nye løysingar vert sett i drift. Om den uakseptable risikoen gjeld ei behandling, teneste, prosess eller eit system som allereie er satt i drift, må systemeigar vurdere om det er naudsynt å stoppe løysinga inntil naudsynte risikoreduserande tiltak er innført. Om løysinga

likevel vert vidareført i ei periode inntil tilstrekkelege risikoreduserande tiltak er gjennomført skal personvernombodet og sikkerheitsforum informerast.

## 6 Implementering og revidering

Det er personalleiar som har ansvaret for at denne retningslinja er kjend hjå dei tilsette. Retningslinja vert evaluert kontinuerleg, og mynde for avgjerd om endringar ligg hjå Sikkerheitsforum i Voss herad.

## 7 Referansar og vedlegg

Lenker til dei mest aktuelle lovar, dokument og rutinar.

- «Lov om offentlege anskaffingar (anskaffingslova)» https://lovdata.no
- «Internkontroll i Voss herad»
- «Handbok for innføring av forvaltningsmodell i Voss herad»
- «Retningslinje anskaffing av IKT løysingar»
- «ROS personvern og informasjonssikkerheit_ MAL 2021»

## Dokument – ID

Utarbeidd av: Innbyggjarservice
Godkjend av/dato:
Revidert:
Neste revisjon:
Saksnummer i 360 online: