Retningslinje for risikostyring for informasjonssikkerhet

Type dokument	Retningslinje
Forvaltes av	Avdelingsleder virksomhetsstyring
Godkjent av	Direktør for Organisasjon og infrastruktur
Gjelder fra	20.06.2023
Neste revisjon	20.06.2025
Unntatt offentlighet	Nei
Referanse ISO	ISO27005:2011
Referanse NSMs Grunnprinsipper for IKT-sikkerhet	1.1.3, 1.1.4, 2.1.10
Referanse LOV/Regel	Personopplysningsloven
Referanse interne dokumenter	Denne retningslinjen er underlagt Politikk for informasjonssikkerhet

1. Formål

Formål med «Retningslinje for risikostyring for informasjonssikkerhet» er å bidra til å forebygge uønskede hendelser eller mangler ved informasjonssikkerheten ved NTNU som kan ha konsekvenser for studenter, ansatte og/eller samfunnet mer generelt.

2. Gjelder for

Retningslinje for risikostyring gjelder for alle som har ansvar for en prosess, prosjekt, eller en anskaffelse, utvikling eller drift av et system. Dette innebefatter ledere, systemeiere, prosesseiere, prosjektledere og forskningsansvarlige.

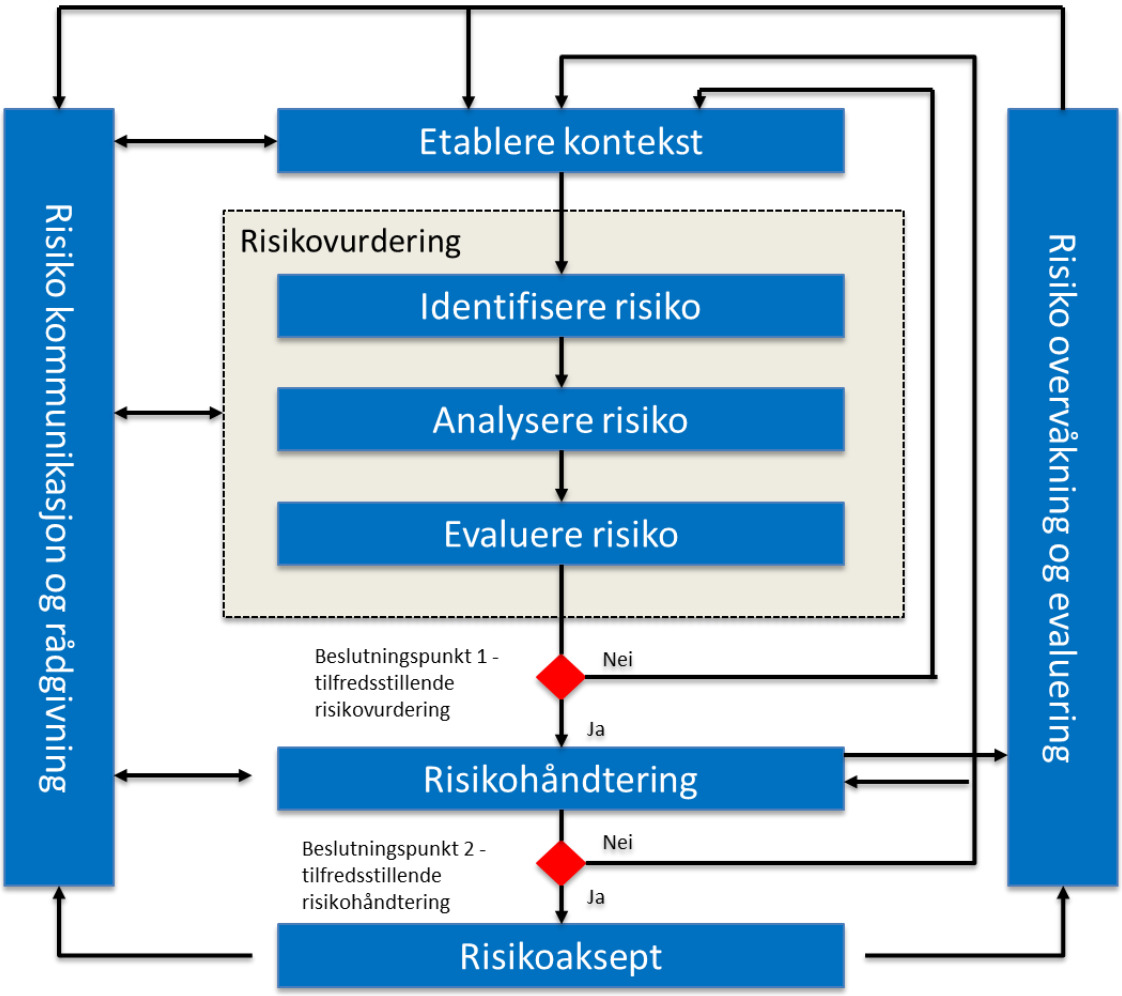
3. Overordnede prinsipper

a. NTNU skal ha en tilnærming til informasjonssikkerhet som er basert på risikovurderinger.
b. NTNUs mål med risikostyring er at risiko skal være vurdert, uakseptabel risiko skal håndteres med tiltak, og resterende risiko skal være akseptert av leder.
c. System og prosesser der informasjonsverdier behandles, skal underlegges risiko – og sårbarhetsanalyser (ROS) minst hvert annet år, og/eller ved vesentlige endringer i organisering, prosesser, IKT-system eller i trusselbilde. Dette for at man skal ha et mest mulig oppdatert bilde av risiko og sårbarhet.

4. Risiko- og sårbarhetsanalyse

Risiko er definert som ett eller flere uønskede scenario beskrevet med kombinasjonen av mulige konsekvenser og tilhørende sannsynlighet. Kontroll av risiko gjøres gjennom risikostyring. Risikostyring et viktig prinsipp i internkontroll og refererer til et samordnet sett av aktiviteter og metoder som brukes til å lede en organisasjon og å kontrollere de mange risikoene som kan påvirke måloppnåelsen.

Risikostyringsprosessen er standardisert gjennom ISO/IEC 27005:2011 standarden og NTNU følger i all hovedsak denne for informasjonssikkerhet, illustrert i figuren under.



a. **Etablere kontekst** for risikovurderingen, dette vil si å bestemme hva som er objekt for vurderingen og hva som ikke inngår. Som en del av dette steget utarbeides risikokriterier spesifikke for den aktuelle risikovurderingen, hvor Konfidensialitet, Integritet og Tilgjengelighet skal inngå.
b. **Risikoidentifisering** for å identifisere og vurdere verdier, trusler og sårbarheter i IKT-systemet eller arbeidsprosessen gjennom tre aktiviteter:
    - Verdivurderingen kommer først siden den bestemmer beskyttelsesbehovet til løsningen, for eksempel ett system som håndterer sensitive persondata vil ha særskilte krav til datahåndtering og det vil sette premisset og sikkerhetsnivået for resten av vurderingen.
    - Neste steg er trusselvurdering med formål å identifisere de mest relevante truslene som er motiverte til å kompromittere informasjonsverdiene våre. En trussel er en risikokilde som vanligvis knyttes til planlagte handlinger i den hensikt å skade systemer eller organisasjon. I tillegg til å estimere truslenes motivasjon og evne for å angripe, skal det vurderes hvor hyppig trusselen kan forekomme hos NTNU.

- Deretter kartlegges og vurderes eksisterende sikkerhetsmekanismer (kontroller og tiltak) i løsningen. Kontroller og tiltak vurderes opp mot hvilke verdier som skal beskyttes.
- Neste steg er å identifisere og vurdere sårbarheter i IKT-systemet eller arbeidsprosessen som kan utnyttes av en trussel for å få tilgang til en verdi.
- Resultatene av verdi, trussel og sårbarhetsaktivitetene nyttes til å identifisere risikoen som foreligger, og hvilke uønskede hendelser og konsekvenser dette kan føre til (risikoscenario).

c. **Risikoanalyse** gjennomføres for å estimere konsekvens og tilhørende sannsynlighet av identifiserte scenarier. Analysen skal avdekke hvilke risikoer som er mest alvorlige og må prioriteres.
d. **Første beslutningspunkt** blir da om risikovurderingen er dekkende nok til å gå videre. I noen tilfeller kan de som gjennomfører risikovurdering ha avdekket områder med stor usikkerhet og må derfor gjøre en grundigere undersøkelse for å oppnå en tilfredsstillende risikovurdering.
e. **Risikohåndtering** er prosessen for å modifisere risiko med den hensikt å gjøre den akseptabel. Håndteringen gjennomføres ved å velge tiltak som kan redusere risikoen til et akseptabelt nivå. Det er i hovedsak fire tilnærminger til å håndtere risiko: (i) redusere risiko, (ii) unngå risiko, (iii) overføre/dele risiko, og (iv) akseptere risikoen som den er. Beslutning for prioritering av tiltak blir tatt på bakgrunn av kost-nytte analyse, hvor effekten i form av risikoreduksjon og kostnaden av tiltaket er vurdert. Det er også i noen tilfeller mulig å øke risikoen for å kunne dra nytte av en mulighet.
f. **Risikoeier (Ansvarlig leder i linjen) vurderer om restrisikoen er akseptabel**. Hvis risikoeier ikke aksepterer risikoen som er igjen etter at det er gjennomført planlagte risikoreduserende tiltak, må nye tiltak vurderes og gjennomføres frem til akseptabel risiko er oppnådd.
g. **Risiko-overvåkning og evaluering**. Risikovurderingen revideres hvert andre år og ved store endringer av systemet eller prosessen.

4.1 Risikokriterier

Risikokriterier er de kriterier som legges til grunn ved beslutning om akseptabel risiko. Slike kriterier kan være uttrykt med ord, være tallfestet eller basert på en kombinasjon. Kriteriene er basert på forskrifter, standarder, erfaringer og/eller teoretisk kunnskap.

a. Ved risikovurderinger skal det utarbeides kriterier innenfor konfidensialitet, integritet og tilgjengelighet.
b. Følgende konsekvenser ved brudd på informasjonssikkerheten skal vurderes:
    i. Skade på materiell eller personer
    ii. Økonomi
    iii. Omdømme
    iv. Personvern

4.2 Aksept av risiko

Akseptabel risiko er risiko som aksepteres i en gitt sammenheng basert på gjeldende verdier i organisasjonen. Hva som er akseptabelt kan endres over tid og variere mellom områder. Det defineres en grense for hva som er uakseptabel risiko basert på risikokriterier. Risiko som anses som uakseptabel bør reduseres så mye som praktisk mulig. Som regel vil det være en nytte-/kostnadsvurdering som

avgjør hva som oppfattes som praktisk mulig, det vil si om, og i hvilken grad, risikoreduserende tiltak skal gjennomføres.
Aksept av risiko må forelegges og besluttes av linjeleder. Linjeleder kan akseptere risiko som gir en konsekvens innenfor hva egen enhet kan tåle. Ved konsekvens utover dette skal aksept av risiko forelegges oppover i linjen. Aksept av risiko gjøres ved å godkjenne ROS med dato. Dato for signering setter gyldighetsperioden for ROS.
Ved identifisering av uakseptabel risiko som kan ha konsekvenser utover omfanget for gjeldende ROS-analyse og/eller medføre store konsekvenser utover egen beslutningsmyndighet, så skal denne risikoen rapporteres oppover i linjen.
Risiko som ikke aksepteres:

a. Konsekvenser som fører til brudd på lover og regler.
b. Konsekvenser som kan påføre NTNU som organisasjon større skade

4.3 Kontrollpunkter, tiltak og rutiner

a. For alle risikokriterier skal det etableres kontrollpunkter og tiltak som er målbare i forhold til fastsatt risikoaksept.
b. Risikoeier skal ha fastsatte rutiner for evaluering av kontrollpunkter og tiltak.
c. Håndtering av avvik skal være en del av risikohåndteringsprosessen.

4.4 Omfang av risikovurdering

Omfanget av risikovurdering bestemmes ut ifra systemets/prosessens krav til konfidensialitet, integritet og tilgjengelighet.

Nivå	Konfidensialitet	Integritet	Tilgjengelighet
Nivå1	**Åpen** Enkel vurdering av risiko for å sikre at det er riktig nivå.	**Lav:** Enkel vurdering av risiko for å sikre at det er riktig nivå.	**Lav:** Enkel vurdering av risiko for å sikre at det er riktig nivå.
Nivå 2	**Intern:** Enkel vurdering av risiko og nødvendige risikoreduserende tiltak.	**Moderat:** Enkel vurdering av risiko og nødvendige risikoreduserende tiltak.	**Moderat:** Enkel vurdering av risiko og nødvendige risikoreduserende tiltak.
Nivå 3	**Fortrolig:** Gjennomføre risiko- og sårbarhetsanalyse og nødvendige risikoreduserende tiltak iht. analysen. Vurdere ekstra krav til tilgangsstyring, logging og revisjon.	**Høy:** Gjennomføre risiko- og sårbarhetsanalyse og nødvendige risikoreduserende tiltak iht. analysen. Vurdere ekstra krav til verifisering av informasjonen, f. eks sjekksum. Vurdere ekstra krav til tilgangsstyring, logging og revisjon.	**Høy:** Gjennomføre risiko- og sårbarhetsanalyse og nødvendige risikoreduserende tiltak iht. analysen. Vurdere ekstra krav til lastbalansering, redundans og restore.
Nivå 4	**Strengt fortrolig:** Gjennomføre risiko- og sårbarhetsanalyse og nødvendige risikoreduserende tiltak iht. analysen.	**Svært høy:** Gjennomføre risiko- og sårbarhetsanalyse og nødvendige risikoreduserende tiltak iht. analysen. Vurdere ekstra krav til verifisering av informasjonen, f.eks. sjekksum.	**Svært høy:** Gjennomføre risiko- og sårbarhetsanalyse og nødvendige risikoreduserende tiltak iht. analysen.

	Vurdere ekstra krav til tilgangsstyring, logging og revisjon, f.eks. multi-faktor autentisering.	Vurdere ekstra krav til tilgangsstyring, logging og revisjon.	Vurdere ekstra krav til lastbalansering, redundans og restore.

5. Roller og ansvar

5.1 Direktør for Organisasjon og infrastruktur

a. er ansvarlig for at alt arbeid med informasjonssikkerhet har en tilnærming som er basert på risikostyring
b. er ansvarlig for utarbeidelse av overordnede akseptkriterier informasjonssikkerhet og at disse er kjent i virksomheten

5.2 Leder av Avdeling for virksomhetsstyring

a. er ansvarlig for rapportering i arbeidet med overordnet risikostyring

5.3 Leder av HR- og HMS-avdelingen

a. er ansvarlig for at ledere er kjent med, og har tilstrekkelig kompetanse, til å ivareta sitt ansvar i henhold til denne retningslinjen

5.4 Linjeleder

a. er ansvarlig for at det utformes en risikomatrise med akseptkriterier for sitt virksomhetsområde
b. skal påse at ansatte er gitt tilstrekkelig opplæring til å kunne gjennomføre en risikovurdering
c. skal sørge for at det gjennomføres risikovurdering for sitt virksomhetsområde

5.5 Prosesseier

a. er ansvarlig for at det utformes en risikomatrise med akseptkriterier for arbeidsprosessen
b. er ansvarlig for at det etableres prosess for risikovurdering som en støtteprosess i arbeidsprosessen
c. skal sørge for at det gjennomføres tilstrekkelig risikovurdering av prosessen

5.6 Systemeier

a. er ansvarlig for at det utformes en risikomatrise med akseptkriterier for systemet
b. er ansvarlig for at det etableres prosess for risikovurdering som en støtteprosess ved endringer i systemet
c. skal sørge for at det gjennomføres tilstrekkelig risikovurdering av systemet

5.7 Prosjektleder

a. er ansvarlig for at det utformes en risikomatrise med akseptkriterier for prosjektet
b. er ansvarlig for at det etableres prosess for risikovurdering som en støtteprosess i prosjektet