Retningslinje for avviksmelding og avvikshåndtering innen Informasjonssikkerhet og personvern

Type dokument	Retningslinje
Forvaltes av	Leder av IT-avdelingen
Godkjent av	Direktør for Organisasjon og infrastruktur
Gjelder fra	12.06.2023
Neste revisjon innen	12.06.2025
Unntatt offentlighet	Nei
Referanse ISO	27002: 5.27,6.4,6.8
Referanse NSMs grunnprinsipper for IKT-sikkerhet	4.4
Referanse LOV/Regel	Eforvaltningsforskriften § 15, § 25, Personopplysningsloven
Referanse interne dokumenter	Politikk for informasjonssikkerhet

1. Formål

Formålet med avviksmelding og avvikshåndtering innenfor informasjonssikkerhet og personvern er å håndtere brudd på gjeldende lover, regler samt interne retningslinjer og rutiner.

Et særskilt formål er å sikre effektiv melding til Datatilsynet ved brudd på håndteringen av personopplysninger. Det er også et formål å sørge for at berørte registrerte varsles uten ugrunnet opphold slik at disse kan ivareta sine interesser.

2. Gjelder for

Retningslinje for avviksmelding og avvikshåndtering gjelder for alle som har tilgang til, og/eller bearbeider og forvalter informasjon gjennom NTNUs digitale og analoge informasjonssystemer.

2.1 Avgrensning

Denne retningslinjen avgrenses mot Retningslinje for hendelseshåndtering og krisehåndtering IT.

3. Overordnede prinsipper

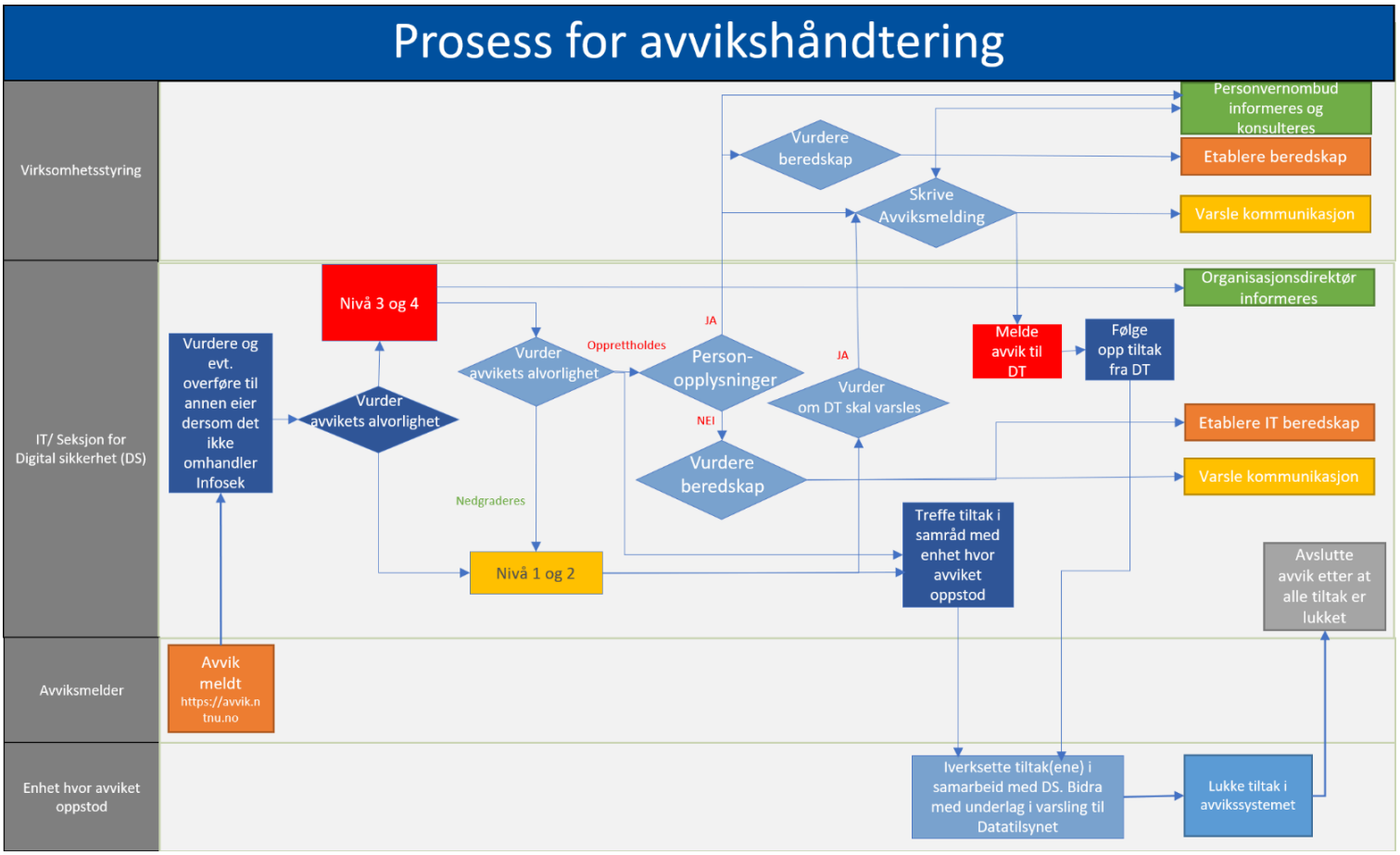
a. Avvikshåndteringen skal bidra til kontinuerlig læring og forbedring av NTNUs rutiner, prosesser og systemer.

b. Meldinger om avvik og avvikshåndteringen utgjør en betydelig del av det systematiske arbeidet med informasjonssikkerhet, og er en viktig del av NTNUs internkontroll.
c. Meldinger om avvik er nødvendig og ønskelig ved NTNU, og alle med tilgang til NTNUs informasjonssystemer har ansvar for å melde avvik ved NTNU.
d. Melding om avvik og håndtering av avvik skal føre til positive konsekvenser for den enkeltes arbeidshverdag og for NTNU som helhet ved at NTNUs arbeidsprosesser og systemer forbedres og effektiviseres.
e. Å reagere på avvik er ikke forbundet med negative sanksjoner. Det betyr at både den som oppdager avviket, og den som melder det inn er beskyttet mot negative reaksjoner.
f. Der resultatet av avviksbehandlingen er knyttet til behandling av personopplysninger skal behandlingen dokumenteres og gjennomgås av ledelsen.

4. Avvikshåndtering

Et avvik er i denne retningslinjen definert som et brudd på lover og regler, samt brudd på NTNUs interne regler, politikk og retningslinjer som regulerer enten direkte eller indirekte, bruken av NTNUs informasjonssystemer, herunder behandling av personopplysninger. Avvikshåndtering er den samlede prosessen med å avdekke, melde, behandle, rapportere status på, samt lukke avviket. Håndteringen skal gjøre det mulig å gjenopprette tilstanden, fjerne årsaken til avviket, redusere negative konsekvenser for både NTNU og tredjepersoner, samt lettere unngå fremtidige informasjonssikkerhetsbrudd og brudd på personvernet. På den måten bidrar avvikshåndteringen til kontinuerlig læring og forbedring av NTNUs rutiner, prosesser og systemer.

Under ligger et visuelt flytdiagram av avvikshåndteringen ved NTNU.



4.1. Melde avvik

a. Den eller de som oppdager avvik skal melde avviket i NTNUs digitale avvikssystem uten unødvendig opphold.

b. Hvilke kategorier skal avviksmeldes:
   - Brudd på lover, regler og instrukser
   - Brudd på retningslinjer, rutiner eller prosedyrer for sikker behandling av informasjon
   - Brudd på personopplysningssikkerheten
   - Manglende rutiner og prosedyrer for korrekt informasjonsbehandling og ivaretakelse av informasjonssikkerheten
   - Manglende rutiner for ivaretakelse av personopplysningssikkerhet
   - Manglende sikkerhetskontroller iht. retningslinjer
   - Manglende tilgangskontroll til informasjonsverdier eller utstyr som benyttes til informasjonsbehandling

4.2. Meldingens innhold

a. Innholdet i avviksmeldingen skal, ved å benytte åpen og intern informasjon, beskrive at det har skjedd et brudd, beskrive hvor bruddet har forekommet. Innholdet skal også beskrive hva som eventuelt er konsekvensen av bruddet.
b. Avviksmeldingen skal ikke inneholde personopplysninger knyttet til navn eller annen type informasjon der det kan være behov for konfidensialitet.
c. Avvik skal aldri rettes mot person, men mot det elementet eller handlingen i arbeidsprosessen som forårsaket sikkerhetsbruddet. Handlingen er «subjektet» i avviket, ikke personen.
d. Avvik som omhandler varsel om kritikkverdige forhold i arbeidet med informasjonssikkerhet skal registreres og håndteres i tråd med NTNUs rutiner for varsling iht. arbeidsmiljøloven.

4.3. Oppfølging av avvik

a. Avviket mottas av Seksjon for digital sikkerhet (SDS) som vurderer avvikets kritikalitet (*lav (1), moderat(2), høy(3), svært høy(4)*).
b. Seksjon for Digital sikkerhet påser at det treffes nødvendige strakstiltak og at de ansvarlige blir varslet.
c. Ved brudd på personvern, se punkt 4.4
d. Avvikseier skal i samråd med avviksbehandler etter beste evne kartlegge og analysere årsaken til avviket for å forsøke å finne rotårsak. Avvikseier er den linjeleder som eier arbeidsutførelsen som avviket gjelder. Kartleggingen gjør at det kan utvikles målrettede og effektive tiltak knyttet til både kompetanse, ressurser, ledelse og rutiner. Ved alle avvik hvor kritikaliteten anses som *lav* (1) eller *moderat* (2), skal avvikseier i linjen være ansvarlig for å håndtere og lukke avviket. Anses kritikaliteten til å være *høy* (3) eller *svært høy* (4) skal avvikseier være organisasjonsdirektør eller på tilsvarende nivå.
e. Der avviket vurderes som *alvorlig*/*kritisk*, vil linjeleder ved den enhet der avviket oppstod være tiltakseier, og må sørge for at nødvendige og umiddelbare pålagte tiltak blir gjennomført.
f. Med utgangspunkt i årsaksfaktorer skal avvikseier vurdere hvordan avviket bør håndteres, og utforme forslag til tiltak. Seksjon for Digital sikkerhet skal i samråd med avvikseier dokumenter foreslåtte tiltak i avvikssystemet med fastsatt frist og ansvarlig person for implementering av tiltak, en tiltakseier. Tiltakseiere kan være en eller flere systemeiere, prosesseiere, ledere på et annet nivå eller annen enhet, eller tiltakseier og avvikseier kan i noen tilfeller være samme person. Tiltakene skal konkretisere ønsket effekt.
g. Tiltakseier skal vurdere foreslåtte tiltak. Ved tiltak som medfører omfattende endringer eller ressurser, skal tiltakseier utforme forslag til løsning med et grovt estimat for ressursbehov. Dette godkjennes av avvikseier før tiltak iverksettes.
h. Tiltakseier rapporterer fremdrift på implementering av tiltaket til avvikseier i avvikssystemet, samt når tiltak er implementert.
i. Ledere ved NTNU skal ta opp avvik klassifisert som *alvorlig* eller *kritisk* i sine ledermøter, og benytte avvikshåndtering som en betydelig faktor i forbedringsarbeidet i sin del av virksomheten. Alle avvik knyttet til håndtering av personopplysninger skal behandles i ledermøter.

4.4. Brudd på personvern

a. Dersom avviket gjelder brudd på personopplysningssikkerheten hvor det er risiko for negative personvernkonsekvenser for den registrerte, eller at størrelsen av avviket er betydelig, skal datatilsynet varsles innen 72 timer.
b. Jurist og personvernombud skal være kopiert på avviksmeldingen der det gjelder mulig brudd på personopplysningssikkerheten.
c. Varsling til datatilsynet
    - Seksjon for Digital sikkerhet (SDS) skal i samråd med jurist og/eller personvernombud vurdere om avviket skal meldes til Datatilsynet. Ved fravær av jurist skal SDS vurdere om avviket skal meldes til Datatilsynet.
    - Jurist skriver varsel til Datatilsynet i samarbeid med SDS og avvikseier, og i samråd med personvernombudet. Ved fravær av jurist utformer SDS og personvernombud varselet.
    - Linjeleder ved den enhet der avviket oppstod, vil være tiltakseier, og skal sørge for å sende inn rapport til SDS som underlag til samlerapport.
d. Ved brudd på personopplysningssikkerheten, og slikt avvik som kan innebære en høy risiko for de registrertes rettigheter og friheter, må avvikseier/tiltakseier iverksette umiddelbare tiltak for å varsle de registrerte slik at de kan ivareta sine interesser. Varselet skal inneholde:
    - Klar og tydelig beskrivelse av arten til bruddet på personopplysningssikkerheten
    - Kontaktopplysning til personvernombud
    - Sannsynlige konsekvenser
    - Beskrive skadebegrensende tiltak som er iverksatt eller planlagt iverksatt
    - Varslingen skal gjøres av tiltakseier og utan ugrunnet opphold etter å ha blitt kjent med avviket.

4.5. Lukking av avvik

a. Avvik lukkes av avviksbehandler når tiltakene er implementert/gjennomført av tiltakseier, og fungerer etter hensikten. Avvik kan også lukkes ved mer omfattende og langsiktige tiltak som ennå ikke er implementert, men som er akseptert og planlagt iverksatt av tiltakseier.
b. Avvikseier aksepterer ferdigstilte tiltak. SDS lukker avviket i samråd med avvikseier.
c. Avviket kan lukkes også når ikke alle tiltak er ferdig implementert hvis kortsiktige tiltak for å begrense skadevirkning er implementert. Det forutsettes at korrigerende tiltak er påstartet, men er av et omfang som det vil ta lang tid å få ferdig implementert.
d. Avvikseier rapporterer til avviksmelder at avviket er lukket.
e. Avvikseier rapporterer til IT-avdelingen om ønskede og oppnådde effekt av avvikshåndteringen.
f. Ved avvik som gjelder personopplysninger, og som er meldt til Datatilsynet, skal tilbakemeldinger fra Datatilsynet registreres på egen sak i ephorte, saksnr 2018/43111. Jurist i avdeling for virksomhetsstyring eller SDS orienterer organisasjonsdirektør og linjeleder om utfallet. Avviksmelder gjøres kjent med tilbakemeldingen når avviket lukkes av SDS.

5. Roller og ansvar

5.1. Rektor

a. er ansvarlig for å fremlegge årlig rapport om informasjonssikkerhet og avviksmeldinger for NTNUs styre

5.2. Direktør for Organisasjon og infrastruktur

a. er ansvarlig for at NTNU har en prosess for å håndtere avvik innen informasjonssikkerhet
b. er ansvarlig for at avvikshåndtering inngår i ledelsens årlige gjennomgang av arbeidet med informasjonssikkerhet
c. er avvikseier ved alvorlige eller kritiske brudd på personvernet

5.3. Linjeleder (avvikseier)

a. er ansvarlig for at ansatte har kunnskap om når og hvordan avvik skal meldes
b. er ansvarlig for at avvikshåndtering er en del av forbedringsarbeidet ved egen enhet
c. er avvikseier og ansvarlig for en forsvarlig håndtering av avvik ved egen enhet
d. er ansvarlig for at tiltak distribueres til tiltakseier for implementering.
e. er tiltakseier i de tilfeller overordnet nivå er avvikseier
f. er ansvarlig for å trekke inn nødvendig bistand ved behov
g. skal analysere avviket, vurdere hvordan avviket bør håndteres og utforme forslag til tiltak for å lukke avviket.
h. er ansvarlig for å sørge for varsling til de registrerte dersom personopplysninger kan være på avveie

5.4. Leder av Avdeling for virksomhetsstyring

a. er ansvarlig for at avvikssystem knyttet til informasjonssikkerhet inngår som en del av NTNUs helhetlige internkontroll og virksomhetsstyring
b. er ansvarlig for at NTNU har et digitalt avvikssystem for meldinger og håndtering av avvik
c. er ansvarlig får å tilrettelegge for innsamling og analyser av data som viser at NTNU har en tilfredsstillende avvikshåndtering
d. er ansvarlig for arbeidet med avvikshåndtering ved underlagt intern/ekstern revisjon
e. skal konsulteres ved endringer i denne retningslinjen

5.5. Leder av HR- og HMS-avdelingen

a. er ansvarlig for at det legges til rette for og tilbys målrettet opplæring innenfor avviksprosessen for ledere og ansatte slik at avvikshåndtering skjer i henhold til denne retningslinjen
b. skal konsulteres ved endringer i denne retningslinjen

5.6. Leder av IT-avdelingen

a. er ansvarlig for mottak, vurdering, fordeling og rapportering av avviksmeldinger
b. skal vurdere om ønskede effekter av avvikshåndteringen er oppnådd

5.7. Leder av Seksjon for digital sikkerhet

a. er ansvarlig for ressurser til å sikre forsvarlig mottak og videreformidling av avvik innen informasjonssikkerhet
b. skal konsulteres ved endringer i denne retningslinjen
c. er ansvarlig for avviksbehandling innenfor informasjonssikkerhet og personvern

5.8. Ansatte og studenter

a. er ansvarlige for å melde avdekkede avvik inn i avvikssystemet i henhold til denne retningslinjen

5.9. Tiltakseier

a. er ansvarlig for implementering av de tiltak som avvikseier har utformet.
b. skal melde til avvikseier når tiltak er implementert, eller det er en plan for implementering over tid.

5.10. Personvernombud

a. skal påse at NTNUs retningslinje om avvikshåndtering følges
b. skal påse at NTNU overholder sine forpliktelser om å varsle Datatilsynet og de registrerte