



ÅRSRAPPORT

SIKKERHET BEREDSKAP 2024



NTNU

Norges teknisk-
naturvitenskapelige universitet



Innhold

1. Sammendrag	5
2. Innledning	7
2.1 Formål	7
2.2 Rammer og betingelser for sikkerhetsarbeidet	7
3. Årsberetning for sikkerhetsarbeidet ved NTNU	8
3.1 Risiko- og sårbarhetsanalyse, ROS SoB24	8
3.2 Nasjonal sikkerhet	9
3.3 Samfunnssikkerhet	12
3.4 Informasjonssikkerhet	15
3.5 Personvern	18
3.6 Hendelser og avvik ved NTNU i 2024	21
3.7 Sikkerhetsmyndighetenes risiko- og trusselvurderinger	23
4. Anbefalte prioriteringer for 2025	25
4.1 Prioriteringer innen nasjonal sikkerhet	26
4.2 Prioriteringer innen samfunnssikkerhet	29
4.3 Prioriteringer innen informasjonssikkerhet	30
4.4 Prioriteringer innen personvern	31

Årsrapporten dekker NTNUs helhetlige sikkerhetsarbeid
innen sikkerhetsområdene:

NASJONAL SIKKERHET

SAMFUNNSSIKKERHET

INFORMASJONSSIKKERHET

PERSONVERN

1. Sammendrag

Sikkerhetsåret 2024 var preget av økende geopolitisk uro og et tilspisset risikobilde for Norge og for kunnskapssektoren. I denne perioden gjennomførte NTNU flere viktige tiltak innen forebyggende sikkerhet på alle sikkerhetsområdene; nasjonal sikkerhet, samfunnssikkerhet, informasjonssikkerhet og personvern. Tabellen nedenfor gir et overordnet bilde av viktige prosesser og milepæler i det forebyggende sikkerhetsarbeid ved NTNU i 2024. Tabellen oppsummerer også sentrale prioriteringer for sikkerhetsarbeidet i 2025.



*NTNU er underlagt en rekke
lover og bestemmelser
som har til hensikt å gjøre
organisasjonen i stand til å
håndtere risiko og farer, og
unngå skade eller tap av verdier.*



2. Innledning

2.1 FORMÅL

Årsrapporten dekker NTNUs helhetlige sikkerhetsarbeid innen sikkerhetsområdene: Nasjonal sikkerhet, samfunnssikkerhet, informasjonssikkerhet og personvern. Rapporten har som formål å oppsummere NTNUs forebyggende sikkerhetsarbeid i 2024. I tillegg gir rapporten et overordnet bilde av hendelser og avvik. Rapporten har videre som formål å presentere nasjonale sikkerhetsmyndigheters trusselvurderinger for 2025, med fokus på trusselvurderingenes betydning for kunnskapssektoren, og for NTNUs sikkerhetsarbeid. Avslutningsvis presenterer rapporten en oversikt over sentrale prioriteringer for NTNUs sikkerhetsarbeid i 2025. Prioriteringene har utgangspunkt i NTNUs overordnede risiko- og sårbarhetsanalyse, ROS SOB24.

2.2 RAMMER OG BETINGELSER FOR SIKKERHETSARBEIDET

Sikkerhet og beredskap ved NTNU reguleres av en rekke eksterne rammebetingelser og forhold. Nasjonale sikkerhetsmyndigheter og Kunnskapsdepartementet stiller krav til hvordan NTNU forholder seg til risiko. NTNU er underlagt en rekke lover og bestemmelser som har til hensikt å gjøre organisasjonen i stand til å håndtere risiko og farer, og unngå skade eller tap av verdier.

Samtidig virker geopolitikk og samfunnsutvikling aktivt inn på risikobildet. Økende geopolitisk ustabilitet har over tid medført en forsterket sikkerhetsorientering i sektoren. Det tilspissede risikobildet, og anbefalingene i NTNUs overordnede risiko- og sårbarhetsanalyse ROS SOB24, har betydning for videre prioriteringer i sikkerhetsarbeidet.

3. Årsberetning for sikkerhetsarbeidet ved NTNU

3.1 RISIKO- OG SÅRBARHETSANALYSE, ROS SOB24

Forebyggende sikkerhetsarbeid skal i henhold til Sikkerhetsloven gjennomføres planlagt og systematisk i form av sikkerhetsstyring. Et nødvendig utgangspunkt for dette er oversikt over risiko og sårbarheter i organisasjonen. NTNU fullførte arbeidet med sin risiko- og sårbarhetsanalyse (ROS SOB24), i juni 2024. Analysen omfatter sikkerhetsområdene samfunnssikkerhet, nasjonal sikkerhet, informasjonssikkerhet og personvern, i tråd med krav fra KD.

ROS SOB24 identifiserer 11 hendelser som er av betydning for evne til drift, kontinuitet, og strategisk utviklingsevne. I tillegg gir analysen oversikt over forebyggende sikkerhetstiltak, samt 6 prioriterte anbefalinger. De fleste anbefalingene fra arbeidet handler om å løfte NTNUs organisatoriske og menneskelige sikkerhetstiltak slik som sikkerhetsstyring, opplæring og bevisstgjøring.

NR	ANBEFALTE TILTAK	STATUS
1	Innføre sikkerhetsstyring som en del av virksomhetsstyringen	Påbegynt
2	Innføre verdioversikt som del av sikkerhetsstyringen	Påbegynt
3	Opplæring som del av sikkerhetsstyringen	Delvis Påbegynt
4	Styrke beredskapskompetansen	Delvis Påbegynt
5	Risikostyring og oppfølging	Påbegynt
6	Innføre felles metodikk for risikostyring	Ikke startet

Tabell 1: Oversikt over anbefalte tiltak og status fra ROS SoB 24

Status for anbefalte tiltak i tabellen er beskrevet nærmere i de kapitlene nedenfor.

3.2 NASJONAL SIKKERHET

NTNU er underlagt [Sikkerhetsloven](#). Loven regulerer nasjonal sikkerhet, og har som formål å forebygge, avdekke og motvirke sikkerhetstruende virksomhet. Store deler av NTNUs forebyggende sikkerhetsarbeid i 2024 handler om ivaretagelse av krav i Sikkerhetsloven. I 2024 har NTNU blant annet gjort organisatoriske endringer i Fellesadministrasjonen som samler sikkerhet og beredskap i én seksjon med fagansvar for nasjonal sikkerhet. Et annet viktig arbeid har vært å utvikle NTNUs styringsdokument for sikkerhet og beredskap. Disse tiltakene svarer ut anbefalinger fra gjennomført internrevisjon i 2023.

3.2.1 Organisatoriske strukturer for sikkerhetsarbeidet

NTNU opprettet i 2024 Seksjon for sikkerhet og beredskap (SoB). Seksjonen er organisert i den nyopprettede avdelingen Avdeling for utvikling og virksomhetsstyring (AUV) i Fellesadministrasjonen (FA). Seksjonen ledes av NTNUs første sikkerhets- og beredskapssjef, som ble tilsatt 1. mars 2024.

Seksjon for sikkerhet og beredskap er tillagt overordnet fagansvar for nasjonal sikkerhet, samfunnssikkerhet og eksportkontroll. Seksjonen har også det faglige ansvaret for NTNUs overordnede risiko- og sårbarhetsanalyse, og koordinering av virksomhetsrapportering knyttet til sikkerhet og beredskap. Fra 2025 har seksjonen også faglig ansvar for å koordinere arbeidet med personvern i NTNU, som følge av omorganisering i Fellesadministrasjonen.

3.2.2 Styringsdokument for sikkerhet og beredskap

Utarbeidelse av NTNUs styringsdokument for sikkerhet og beredskap ved NTNU har vært en viktig prioritering i 2024. Styringsdokumentet var på høring i siste tertial, og ble vedtatt og gjort gjeldende i organisasjonen i februar 2025.

Styringsdokumentet utgjør en viktig ramme for NTNUs sikkerhetsarbeid. Gjennom dette har NTNUs ledelse fordelt roller og ansvar, etablert NTNUs sikkerhetsorganisasjon, og beskrevet sikkerhetsarbeidet i tråd med føringer i Virksomhetssikkerhetsforskriften.

- Styringsdokumentet har som formål å:
- strukturere sikkerhetsarbeidet i henhold til lov- og myndighetskrav, og i tråd med ambisjonen om ett NTNU.
- samle og koordinere sikkerhetsressurser i hele NTNU, som innbefatter alle fakulteter, campuser, Vitenskapsmuseet, og Fellesadministrasjonen.
- beskrive roller, myndighet og ansvar i NTNUs forebyggende sikkerhetsarbeid som er kritiske for å sikre effektiv implementering og vedlikehold av sikkerhetstiltak ved NTNU.
- bidra til økt kollektiv forståelse for betydning av sikkerhet i NTNU

NTNU har en rekke retningslinjer og politikker som til sammen utgjør en del av NTNUs styringssystem for sikkerhet og beredskap. Styringsdokumentet supplerer disse eksisterende dokumentene, og sikrer at NTNU har et komplett formelt styringssystem for sikkerhet.

3.2.3 Sikkerhetsrapportering

NTNU innførte sikkerhet og beredskap som tema i NTNUs overordnede virksomhetsrapportering i siste tertial av 2024. Rapporteringen skal bidra til at NTNU løpende fanger opp behov for endringer i sikkerhetsarbeidet, og gjøre NTNU i stand til å rapportere til nasjonale sikkerhetsmyndigheter om sikkerhetstilstand og forebyggen- de sikkerhetsarbeid.

3.2.4 Personellsikkerhet

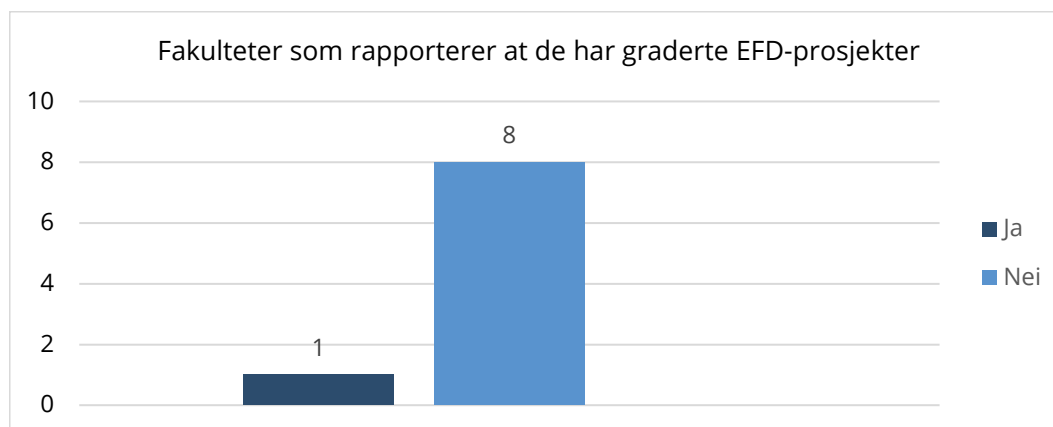
Virksomheter under KD som håndterer sikkerhetsgradert informasjon og/eller skjermingsverdige objekter og infrastruktur må ha ansatte som er autorisert. Personer som autoriseres for tilgang til informasjon gradert KONFIDENSIELT eller høyere, må ha gyldig [sikkerhetsklarering](#).

Før virksomheter under KD selv kan autorisere egne ansatte må:

- Virksomheten ha et dokumentert styringssystem for sikkerhet, jf. [Virksomhetssikkerhets-forskriften](#)
- Virksomhetsleder og/eller den autorisasjonsansvarlige være autorisert av KD

Disse kriteriene er nå oppfylt for NTNU, slik at NTNU kan autorisere ansatte. I vedlegg til NTNUs styringsdokument er det etablert rutiner for personellsikkerhet som gjør NTNU i stand til å forvalte dette på en god måte. NTNU har delegert autori- sasjonsansvaret fra Rektor til Seksjon for sikkerhet og beredskap.

Behovet for autorisering av ansatte har i 2024 vist seg nødvendig for blant annet å muliggjøre NTNUs deltakelse i et gradert European Defence Fund (EDF) prosjekt. Det kan bli behov for ytterligere autorisering i forbindelse med eventuelle tilslag på nye graderte prosjekter.



Figur 1: Fakulteter som rapporterer at de har graderte EFD-prosjekter. Kilde: årsrapportering 2024

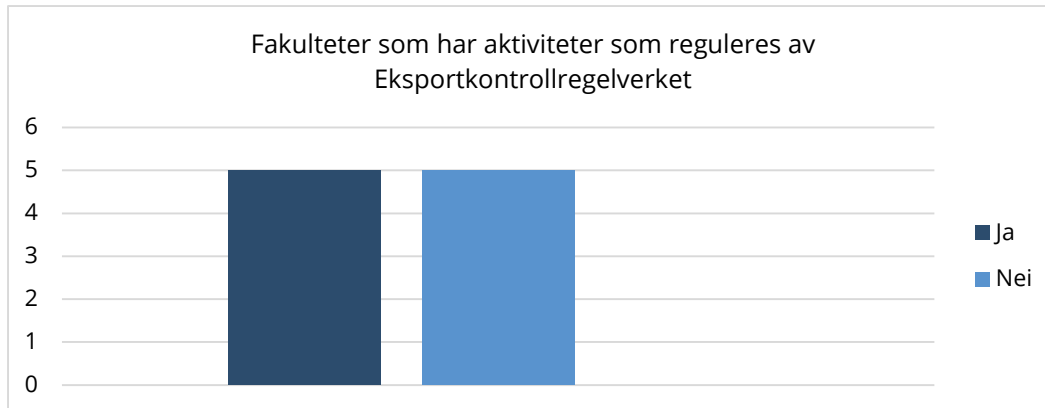
3.2.5 Verdikartlegging

Høsten 2024 gjennomførte NTNU en pilot innen verdikartlegging. Kartleggingen omhandlet informasjonsverdier ved et institutt ved NV-fakultetet. Formålet med piloten var å teste en prosess og metode for verdikartlegging ved et av de større fakultetene ved NTNU, for å innhente innsikt om hvordan NTNU kan arbeide med verdikartlegging. NTNU vil bruke erfaringer fra piloten i det videre arbeidet med verdikartlegging i organisasjonen.

3.2.6 Eksportkontroll

Hovedvekten av NTNUs fakulteter har aktiviteter som faller inn under eksportkontrollregelverket. I tillegg har flere av avdelingene i Fellesadministrasjonen aktiviteter som må vurderes i lys av regelverket, slik som eksempelvis rekruttering av ansatte, innkjøp av systemer, og deler av IT-avdelingens ansvarsområder.

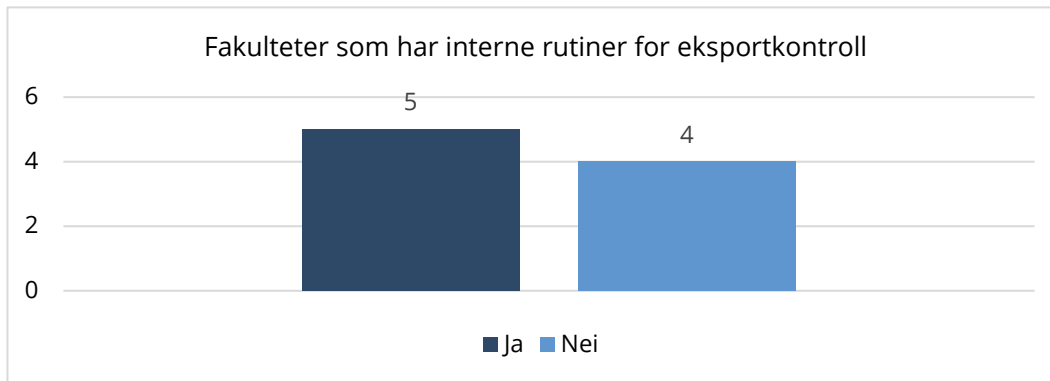
NTNUs ekspertise på eksportkontroll har frem til 2024 vært lokalisert ved de teknologiske fakultetene. Disse fakultetene har bygget opp spesialisert kompetanse på feltet, og flere av fakultetene har etablert interne rutiner for eksportkontroll.



Figur 2: Fakulteter som har aktiviteter som reguleres av Eksportkontrollregelverket. Kilde: Årsrapportering 2024

I 2024 ble det etablert en ny stilling for fagansvar innen eksportkontroll. Mange enheter ved NTNU har erfart at eksportkontrollregelverket utfordrer NTNU. Regelverket er komplekst, og krever spesialistkompetanse. I 2024 ble det derfor opprettet en ny stilling med fagansvar for eksportkontroll, tilknyttet Seksjon for sikkerhet og beredskap. Til stillingen ligger det et ansvar for å styrke evnen til systematisk etterlevelse i hele NTNU. I samme periode har NTNUs eksportkontrollklynge blitt utvidet til 28 medlemmer. Flertallet av NTNUs fakulteter deltar i klyngen, som er en viktig informasjons- og diskusjonsarena.

Seksjon for sikkerhet og beredskap arrangerte i samarbeid med PST Trøndelag en workshop innen eksportkontroll høsten 2024. Målsetningen var forebygging av uønsket teknologioverføring, samt å øke kompetansen i organisasjonen innen eksportkontroll.



Figur 3: Fakulteter som har interne rutiner for eksportkontroll. Kilde: Årsrapportering 2024

NTNU er medlem av [EECARO](#), som har som mål å spre kunnskap om eksportkontroll slik at europeiske universiteter skal bli i stand til å etterleve krav fra myndighetene. EECARO gjennomfører et årlig seminar, og flere av NTNUs fakulteter deltok på dette i 2024. EECARO arrangerer også nettbasert undervisning. Seksjon for sikkerhet og beredskap planlegger en ny workshop i eksportkontroll i løpet av 2025 med representanter fra EECARO som instruktører.

NTNU benytter E-lisens for søknader og forespørsler om lisens. NTNU har sendt inn 9 saker i 2024. I to av sakene ble lisens innvilget. Syv av sakene krevde ingen lisens eller forhåndstillatelse. En sak er ikke avgjort. Søknadene ble behandlet av UD i 2024, og behandles av det nye Direktoratet for eksportkontroll og sanksjoner (DEKSA) fra 2025.

3.2.7 Sikkerhet i internasjonalt samarbeid

NTNUs fagmiljøer er, og skal være, engasjert i det internasjonale kunnskapsfellesskapet. Også i internasjonalt samarbeid er sikkerhetskultur sentralt. NTNU har i løpet av 2024 gjennomført et utvalgsarbeid knyttet til hvordan NTNU skal håndtere krav og forventninger til ansvarlighet i internasjonalt samarbeid. Utvalgets arbeid har vært å avgrense hvordan ansvarlighet i internasjonalt samarbeid kan forstås ved NTNU, med utgangspunkt i akademiske verdier og nasjonale interesser, herunder sikkerhetsinteresser. Utvalgets rapport var på høring i organisasjonen i siste tertial 2024.

3.3 SAMFUNNSSIKKERHET

Samfunnssikkerhet er samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner, og setter liv og helse i fare. NTNU utøver forebyggende arbeid innen samfunnssikkerhet gjennom etablering av beredskapsordninger, sitt beredskapsplanverk og beredskapsøving. Videre håndterer NTNU konkrete hendelser gjennom aktivt beredskapsarbeid.

3.3.1 Anskaffelse av beredskapsverktøy (Rayvn)

NTNU har siden 2020 benyttet beredskapsverktøyet CIM. CIM var del av en rammeavtale inngått av DSB som NTNU hadde sluttet seg til. Denne rammeavtalen utløp i 2023. DSB inngikk en ny rammeavtale med Rayvn AS/Proactima AS 30. juni 2023. Denne avtalen sluttet NTNU seg til.

NTNU har i løpet av 1. halvår 2024 etablert Rayvn som beredskap- og krisehåndteringsverktøy, og siden medio juni 2024 har Rayvn vært i bruk ved håndtering av beredskapshendelser.

Siden implementeringen har det blitt opprettet 37 ulike typer reelle beredskapshendelser som har blitt håndtert ved NTNU. Antallet reelle hendelser i tidsperioden tilsier at det i snitt forekommer hendelser hver 5 dag ved NTNU.

3.3.2 Beredskapshendelser og øving

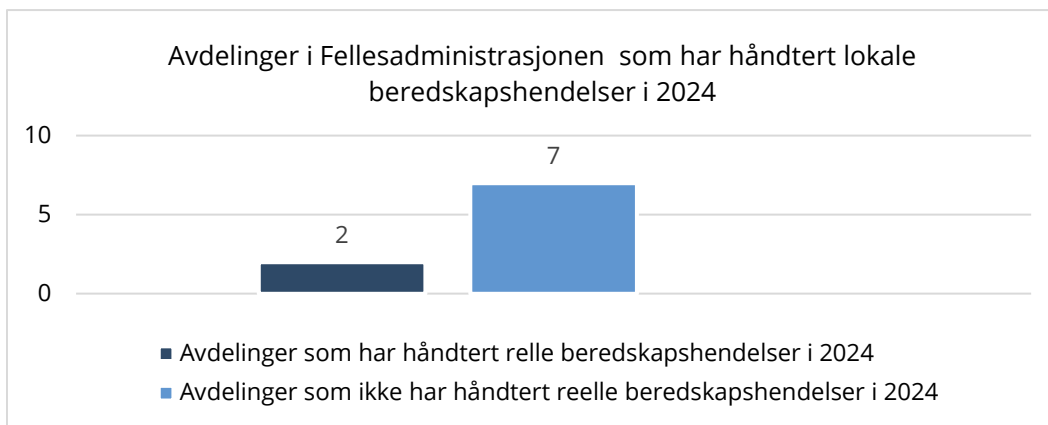
Flertallet av NTNUs fakulteter har håndtert reelle beredskapshendelser på lokalt nivå i 2024. Til sammenlikning har det vært et mindretall lokale beredskapshendelser ved Avdelingene i Fellesadministrasjonen i samme periode. Hendelsene som har funnet sted har vært innenfor følgende definerte hendelseskategorier, jf. NTNUs beredskapsplan:

DFU 01 – Savnet/skade/dødsfall – student, ansatt eller besøkende

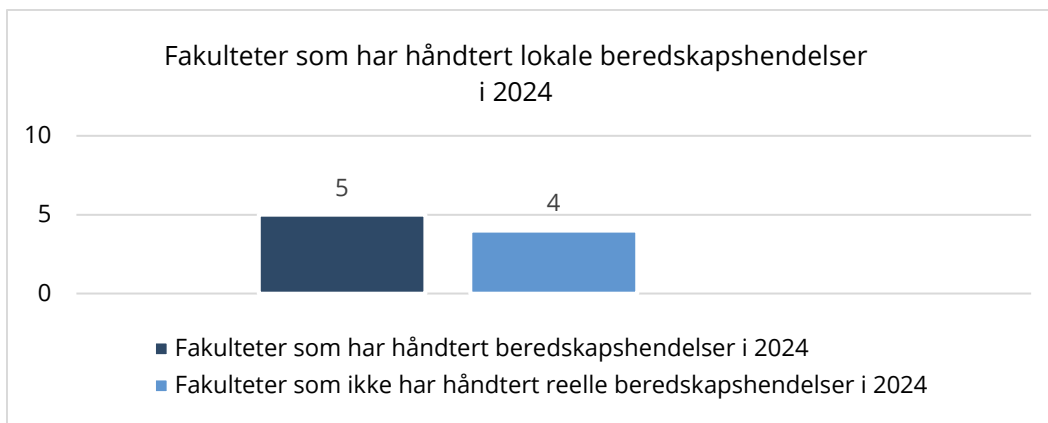
DFU 05 - Informasjonssikkerhetshendelse

DFU 06 - Brann, eksplosjon og evakuering

DFU 11 - Omdømmehendelse



Figur 4: Avdelinger i Fellesadministrasjonen som har håndtert lokale beredskapshendelser i 2024. Kilde: årsrapportering 2024



Figur 5: Fakulteter som har håndtert lokale beredskapshendelser i 2024. Kilde: årsrapportering 2024

Flertallet av NTNUs fakulteter har gjennomført lokale beredskapsøvelser i 2024. Det er også gjennomført øvelser i flere av avdelingene i Fellesadministrasjonen. Samvirke med eksterne samarbeidspartnere, slik som SINTEF, har inngått i noen av øvelsene.

Gjennomførte øvelser har vært innenfor følgende definerte hendelseskategorier, jf. NTNUs beredskapsplan:

DFU 1 – Savnet/skade/dødsfall – student, ansatt eller besøkende

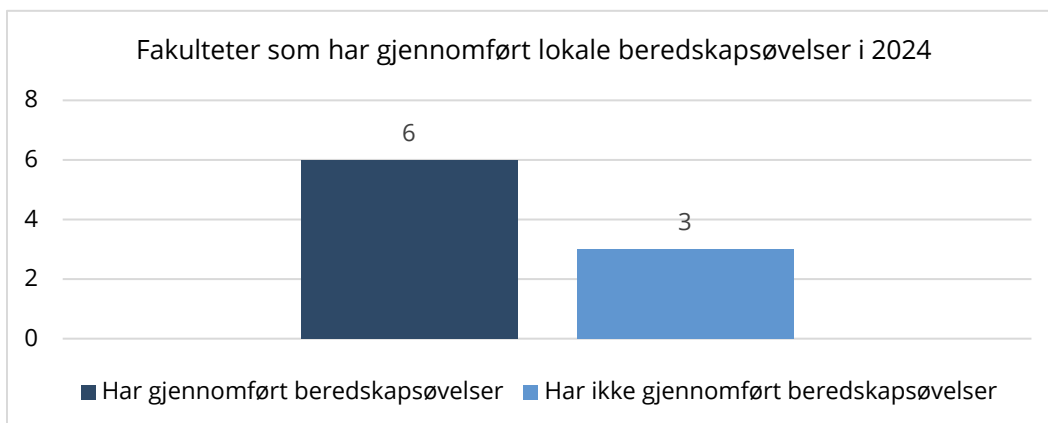
DFU 2 – Hendelse i utlandet

DFU 5 – Informasjonssikkerhetshendelse

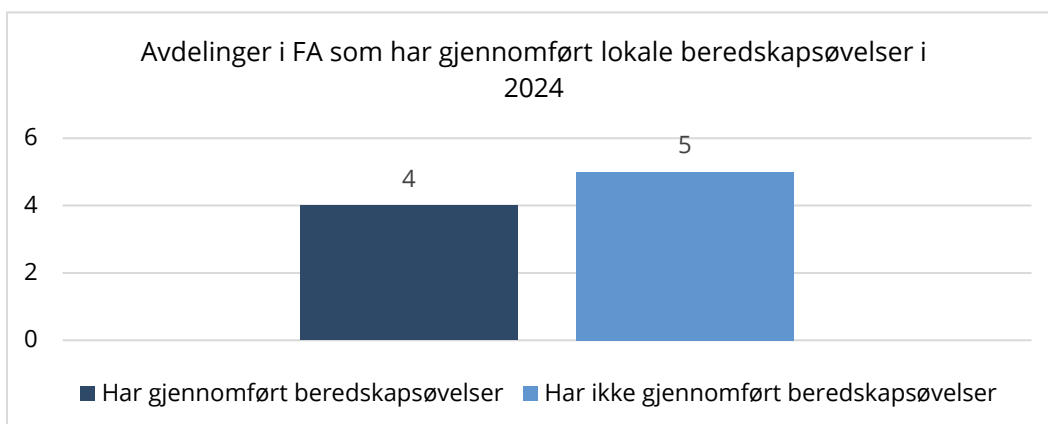
DFU 6 – Brann, eksplosjon og evakuering

DFU 11 – Omdømmehendelse

Både fakultetene og avdelingene i Fellesadministrasjonen rapporterer om at hovedvekten av enhetene har tilstrekkelig kompetanse til å håndtere beredskapshendelser lokalt. Behov for samtrening med andre, ytterligere opplæring og øvelser trekkes samtidig frem som viktig. Mange av enhetene har lokalt planverk som supplerer NTNUs beredskapsplanverk og som er til hjelp i lokal beredskapshåndtering.



Figur 6: Fakulteter som har gjennomført lokale beredskapsøvelser i 2024. Kilde: Årsrapportering 2024



Figur 7: Avdelinger i FA som har gjennomført lokale beredskapsøvelser i 2024. Kilde: Årsrapportering 2024

3.3.3 Obligatorisk opplæring innen livstruende tilsiktede handlinger

Et av scenarioene som er beskrevet i ROS-SoB 2024 er livstruende tilsiktede handlinger som kan medføre alvorlig skadde og i ytterste konsekvens tap av liv. Scenarioet omfatter tilsiktede handlinger; masseangrep og «skoleangrep».

NTNUs styre fattet høsten 2024 et vedtak om gjennomføring av obligatorisk opplæring for ansatte om forebygging og håndtering av livstruende hendelser. Opplæringen ble satt sammen av eksisterende digitale ressurser fra Sikresiden.no. Læringsmål var handlingskompetanse i møte med livstruende vold, og det å gjøre seg kjent med sine omgivelser i et sikkerhetsperspektiv. Alle studenter ble også oppfordret til å ta den samme opplæringspakken.

NTNU har også gjennomført en risikokartlegging knyttet til temaet trakassering, vold og trusler. Dette er gjort som del av oppfølgingen av ARK-prosessen, som er en viktig del av NTNUs systematiske HMS-arbeid. Kartleggingen viser identifiserte risikoer og tiltak som er relevante å iverksette ved de ulike enhetene ved NTNU. Tiltakene sorteres i oppfølgingsansvar ved FA; mellom henholdsvis Seksjon for sikkerhet og beredskap (SoB) og Seksjon for HMS.

3.4 INFORMASJONSSIKKERHET

NTNUs verdier består av informasjon, eller områder, systemer og mennesker som oppbevarer eller behandler informasjon. NTNUs politikk for informasjonssikkerhet definerer mål for informasjonssikkerheten.

3.4.1 Risiko- og sårbarhetsvurderinger av informasjonssystemer

I 2024 har NTNU gjennomført flere risiko- og sårbarhetsvurderinger (ROS) av informasjonssystemer enn tidligere. I 2024 ble det gjennomført omtrent 40 slike risikovurderinger i verktøyet Diri. Dette inkluderer både nye systemer, og systemer som allerede er i bruk. Risiko- og sårbarhetsanalyser innebærer identifisering av risikoreduserende tiltak, som gir grunnlag for prioritering av ressurser. Det ble gjennomført en felles gjennomgang av risikovurderingene for Seksjon for IT-infrastruktur ved IT-avdelingen ved årsslutt.

3.4.2 Gjestetjenesten (GREG)

Personer som skal være tilknyttet NTNU i en avgrenset periode registreres som gjester i NTNUs Gjestetjeneste (GREG). Tjenesten ble innført i 2023, og muliggjør oppfølging av behov for grunnleggende IT-tilganger for eksterne, slik som for eksempel eksterne sensorer eller innleide ansatte fra vikarbyrå.

Ved risikovurdering av tjenesten ble det identifisert flere risikoer, deriblant at gjestebrukere hadde IKT-tilgang i opptil 30 dager etter endt opphold ved NTNU. Det er derfor gjort en administrativ endring i IKT-reglementet i 2024. Endringen medfører at når arbeidsforhold, studierett eller annen form for tilknytning til NTNU opphører, stenges brukertilgangen til NTNUs IKT-infrastruktur.

3.4.3 Tjenesteportefølje

IT-avdelingen har etablert en tjenesteportefølje som synliggjør de forskjellige tjenestenes kritikalitetsnivå og klassifisering. Status og revisjonsdato på risikovurderinger (ROS), personvernkonsekvensvurderinger (DPIA), og eventuell databehandleravtale fremkommer også.

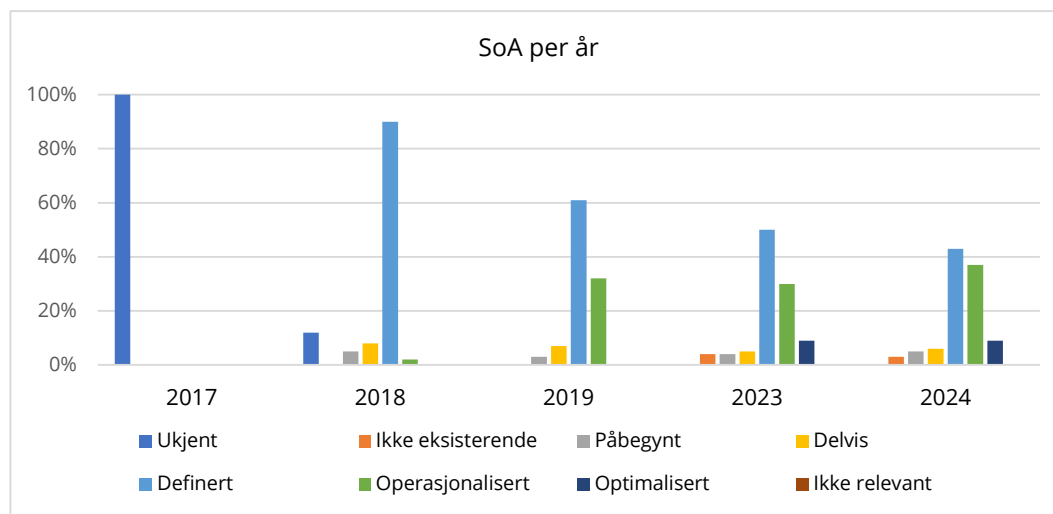
3.4.4 Informasjonssikkerhetsleder

NTNU innførte funksjonen Informasjonssikkerhetsleder i mars 2024. Funksjonen ligger til seksjonsleder ved Seksjon for digital sikkerhet i IT-avdelingen. Informasjonssikkerhetsleder er ansvarlig for å lede det overordnede arbeidet med informasjonssikkerhet gjennom å utvikle, iverksette, og følge opp strategi, politikk, retningslinjer og tiltak for å ivareta informasjonssikkerhet ved NTNU.

3.4.5 Etterlevelse av styringssystem for informasjonssikkerhet og personvern (ISMS)

Mot slutten av 2024 ble det gjennomført en State of Applicability (SOA)-analyse for å sikre at relevante krav i ISO-standarden (ISO27001) er inkludert i styringssystemet, samt for å få en oversikt over endringene det siste året. Analysen viser at noen flere krav har gått fra å være definert til å bli operasjonalisert. Det betyr at det er gjort forbedringer i styringssystemet til NTNU, og krav i ISO-standard som tidligere var definert er i løpet av 2024 blitt implementert og tatt i bruk.

Utrulling av ny infrastruktur og innstramming i brannmur, samt ny sikkerhetsorganisering er blant tiltakene som har medført at flere krav er operasjonalisert.



Figur 8: SOA per år

3.4.6 Opplæring og arrangementer innen informasjonssikkerhet

Obligatorisk opplæring i informasjonssikkerhet

Siden 2023 har alle ansatte og studenter ved NTNU fått tilsendt grunnleggende opplæring i informasjonssikkerhet. Opplæringen er obligatorisk for å sikre et minimumsnivå av kunnskap om informasjonssikkerhet. Informasjon om fullført opplæring lagres i NTNUs brukeradministrative system. Brukere som ikke fullfører opplæringen, får tilsendt påminnelse frem til opplæringen er registrert fullført.

I juni 2024 endret NTNU system for e-læringskurset fra Nanolearning til Nettskjema, i tråd med anbefalinger i årsrapport for sikkerhet 2023. Ved årsslutt 2024 hadde 78 % av NTNUs ansatte og 51 % av NTNUs studenter fullført opplæringen. Dette er tall som baserer seg på aktive brukere ved NTNU.

Sikkerhetsmåneden

Nasjonal sikkerhetsmåned er et konsept koordinert av Norsk senter for informasjonssikring (NorSIS). Arrangementet skjer innenfor rammen av EUs årlige europeiske sikkerhetsmåned. I 2024 ble nasjonal sikkerhetsmåned gjennomført for 14. gang i Norge, og for 7. gang ved NTNU. Formålet med Nasjonal sikkerhetsmåned er å øke engasjement, bevissthet og kunnskap om digital sikkerhet. Årets tema var "våre digitale verdier".

Gjennom en rekke foredrag og artikler ble sikkerhetsarbeidet ved NTNU fremhevet. Viktige fokusområder var å fremme bevissthet om verdier som er beskyttelsesverdige, og hvordan ansatte kan ta en aktiv rolle i å beskytte disse.

Tilbakemeldinger på arrangementene har vært positive, men det har vært registrert lavere deltakelse enn ønsket. For fremtidige arrangement må det vurderes hvordan man bedre kan nå ut til ansatte og skape engasjement rundt aktivitetene.

Fagdag for fagnær IT ved fakultetene ved IV, NV og IE

Våren 2024 arrangerte IV, NV og IE fakultetet to-dagers fagdag for fagnær IT og tekniske ledere ved de nevnte fakultetene. Arrangementet var et samarbeid mellom Seksjon for digital sikkerhet og sikkerhetsledere ved fakultetene, med formål om å skape en felles samling for relasjonsbygging, faglig påfyll og bevisstgjøring.

Arrangementet bestod av en rekke foredrag som omhandlet trusselsituasjonen i Norge og kunnskapssektoren, gjennomgang av hvordan NTNUs Openstack virtualiseringsplattform kan benyttes av fagmiljøene, ressurser fra IT-avdelingen, sikkerhetslogging, hendelser og operativt sikkerhetsarbeid. Arrangementet innebar også en skrivebordsøvelse som handlet om b verktøy for kunstig intelligens (KI). KI-verktøyet var ikke vurdert av IT-avdelingen, og ansatte/studenter med ikke-administrerte pc-er kunne laste ned verktøyet mens vurderingen pågikk. Fagnær IT, som er nærmest fagmiljøene, fikk en rekke problemstillinger om bruk av kunstig intelligens de måtte vurdere.

34 ansatte fra lokal IT/tekniske ledere deltok på fagdagene. Evalueringen viste at over 90 % av deltakerne syntes at det var nyttig eller svært nyttig å delta. Deltakerne ga tilbakemelding om at de ønsket seg mer innsyn i faktiske sikkerhetshendelser og hvilke konkrete trusler vi står overfor i evalueringen.

3.4.7 Utrulling av ny infrastruktur og innstramming i brannmur

I 2024 igangsatte NTNU IT utrulling av nytt ett-campus nett, og utvidelse av kapasitet i nytt datasenter. Målsetningen for disse tiltakene er å etablere en sikrere og mer fleksibel grunnmur for NTNUs tjenester innen forskning og undervisning.

Utrullingen av nytt campusnett skjer gradvis. På denne måten gis organisasjonen rom for å tilpasse seg en ny tilnærming til IT-infrastruktur. Ny infrastruktur inkluderer en sikkerhets- og sonemodell som gir mindre rom for å sette opp systemer på områder som medfører økt risiko for NTNU.

Noen utfordringer har blitt oppdaget som del av utrulling. Ved enkelte institutt anvendes IT-løsninger som tradisjonelt har vært plassert på steder i nettverket som ikke kan videreføres i en effektiv sikkerhets- og sonemodell. Disse utfordringene har blitt løst gjennom midlertidige unntak, i påvente av at IT-avdelingen iverksetter et systematisk arbeid som innebærer å flytte systemene.

Høsten 2024 ble det iverksatt innstramming i NTNUs brannmur. Formålet var å hensiktsmessig plassering av tjenester i IT-infrastrukturen, og forhindre eksponering av tjenester der hvor dette var nødvendig. Dette arbeidet pågår, og vil løpe inn i første kvartal 2025. Arbeidet gjøres for å minimere NTNUs digitale angrepsflate, og for å få kontroll på risiko og sikre tilstrekkelig og god forvaltning av de systemene som skal være eksponert. Alle eksponerte IT-systemer utgjør en risiko for organisasjonen, men ved å kun eksponere systemer som har behov for det, samt å ha fokus på god forvaltning, drift og sikkerhetsmonitorering, vil denne risikoen være håndterbar innenfor et forsvarlig nivå.

3.4.8 Internrevisjon

NTNUs internrevisor, PricewaterhouseCoopers (PwC), har gjennomført seks revisjoner i løpet av 2024, deriblant en oppfølgingsrevisjon for personvern og informasjonssikkerhet. Formålet med revisjonen har vært å bidra til at NTNU får en mer helhetlig organisering, tilnærming og oversikt på områdene.

Revisjonen består av to hoveddeler:

1. Oppfølging av status for det virksomhetsovergrepene informasjonssikkerhets- og personvernarbeidet.
2. En avsjekk av hvordan det arbeides med ivaretagelse av informasjonssikkerhet og personvern på to fakulteter.

Revisjonen er ikke ferdigstilt, blant annet på grunn av omorganisering av Fellesadministrasjonen ved NTNU. Det er ventet at revisjonen blir ferdig i løpet av 2025.

3.5 PERSONVERN

NTNU arbeider systematisk og kontinuerlig med personvern. NTNU skal overholde gjeldende personvernlovgivning og behandle personopplysninger på en trygg og sikker måte. [Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning](#) og styringssignaler fra KD ligger til grunn for kontinuerlig arbeid på feltet.

3.5.1 Status innen personvernområdet

Det ble i 2024 igangsatt en omfattende gjennomgang av anbefalinger fra gjennomførte revisjoner for å kartlegge status på personvernområdet for NTNU. Dette arbeidet har resultert i en oversikt over organisatorisk og regulatorisk etterslep på personvernområdet. Oversikten utgjør et viktig kunnskapsgrunnlag for prioriteringer.

NTNU skal holde oversikt over hvilke personopplysninger som behandles, jf. [Personvernforordningen](#). Dette innebærer å ha oversikt over systemer eller tjenester hvor informasjon og personopplysninger behandles. Videre skal NTNU ha oversikt over hvilke informasjons- og opplysningstyper som behandles, dataflyt og tilganger, og oppfølging av internkontroll for å sikre etterlevelse av regelverket.

I 2024 etablerte NTNU en komplett behandlingsprotokoll for behandling av personopplysninger i administrative saksprosesser. Denne behandlingsprotokollen gir oversikt over behandling av personopplysninger i totalt 376 identifiserte saksbehandlingsprosesser og synliggjør ca 2600 behandlinger i lovens forstand innenfor 81 transaksjonselementer. Det er etablert en plan for videre arbeid med protokollen i

2025 for å sikre at innholdet holdes oppdatert og blir en viktig datakilde for internkontroll av NTNUs administrative saksbehandling.

Når NTNU behandler personopplysninger og står som behandlingsansvarlig, plikter NTNU å ivareta individets rettigheter og friheter. Gjennomføring av [personvernkonsekvensvurderinger \(DPIA\)](#) er viktig for å kvalitetssikre dette. I 2024 har det blitt gjennomført flere personvernkonsekvensvurderinger av viktige tjenester og verktøy, deriblant for Copilot with Commercial Data Protection (tidligere Bing Chat Enterprise), Copilot for Microsoft 365 (overordnet), NTNUs bruk av sosiale medier (overordnet), Elements (saksbehandlingssystem), Rayvn (beredskapssystem), Bevisst (virksomhetsstyringssystem) og Kindly Chatbot (aktiv spørsmålsrobot på NTNUs nettsider).

3.5.2 Informasjon ved behandling av personopplysninger

Når NTNU samler inn og bruker personopplysninger, skal det gis informasjon til de dette gjelder. Personvernforordningen definerer dette som «de registrerte». Informasjon som gis til de registrerte via NTNUs nettsider, personvernerklæringer og retningslinjer for behandling av personopplysninger skal være lett tilgjengelig, forståelig, åpen og tilpasset mottakeren.

I 2024 har NTNU oppdatert den overordnede personvernerklæringen om hvordan NTNU behandler personopplysninger via sine kontoer i sosiale medier. NTNU har også sikret at informasjon er åpent tilgjengelig på NTNUs nettsider for alle ansatte og studenter når verktøy som Copilot har blitt tilgjengeliggjort.

3.5.3 Opplæring

NTNU skal ha en helhetlig opplæringsplan for personvern som sikrer at alle relevante aktører har nødvendig kompetanse.

I 2024 lanserte Forskningsdatahjelpen opplæring for studenter som skal bruke personopplysninger i oppgavene sine. Opplæringen består av fem moduler, basert på videokurs og oppgaver, og er tilgjengelig i H5P for alle studenter.

Som del av sandkasseprosjektet for M365 Copilot er det utarbeidet og gjennomført et opplæringsopplegg innen kunstig intelligens og personvern. Opplæringen ble gjennomført for deltakere fra administrasjonen ved Institutt for datateknologi og informatikk (IDI). Opplæringen er åpent tilgjengelig via prosjektets nettsider.

I tillegg er det gjennomført mindre opplæringstiltak gjennom året, som blant annet innlegg for undervisere som deltar på Unipeds undervisning innen kunstig intelligens.

3.5.4 Avvikshåndtering

NTNU skal ha en robust og effektiv avvikshåndtering, som kontinuerlig forbedrer sikkerhetsnivået og sikringstiltak gjennom systematisk evaluering og læring etter avvik fra rutiner, hendelser og brudd på personopplysningssikkerheten. I 2024 er det identifisert behov for å revidere rutiner for avvikshåndtering, gjennomføre årlig internkontroll av alle innmeldte avvik for å sikre kontinuerlig og systematisk kvalitetsforbedring.

3.5.5 Sandkasse – Pilotere Copilot for Microsoft 365

NTNU har deltatt i [Datatilsynets regulatoriske sandkasse](#) for personvernvennlig innovasjon og digitalisering med prosjektet «Pilotere Copilot for Microsoft 365». Målsetningen med Datatilsynets regulatoriske sandkasse er å stimulere til personvernvennlig innovasjon og digitalisering.

Prosjektet har jobbet etter tre konkrete delmål; utarbeide en verktøykasse for at organisasjoner i offentlig sektor kan bli «Copilot ready», utvikle informasjonsmateriell om hvordan organisasjoner i offentlig sektor kan påvirke leverandører til å tenke operasjonelt personvern tidlig i utvikling av nye tjenester hvor KI benyttes, samt å arrangere et åpent fagseminar for å dele prosjektets funn for alle i offentlig sektor.

NTNU leverte sin sluttrapport i juni 2024. Datatilsynets rapport fra november 2024 fokuserer på personvern og beskriver hvordan man bør gå frem for å kunne ta i bruk M365 Copilot i offentlige organisasjoner. Datatilsynet og NTNU peker på mange av de samme funnene, og rapportene samlet sett er et godt verktøy for andre virksomheter som ønsker å ta i bruk M365 Copilot.

Prosjektet var et samarbeid mellom NTNU, Datatilsynet, Microsoft, Sikt og Crayon. I tillegg deltok flere samarbeidspartnere fra offentlig sektor, som blant annet Statens vegvesen, Vestland fylkeskommune og NAV. Prosjektet har gjennom hele prosjektperioden hatt fokus på erfaringsdeling med andre virksomheter, og har i 2024 holdt 50 foredrag over hele landet for å dele informasjon og erfaringer. Prosjektet var finansiert av Nemonoor.

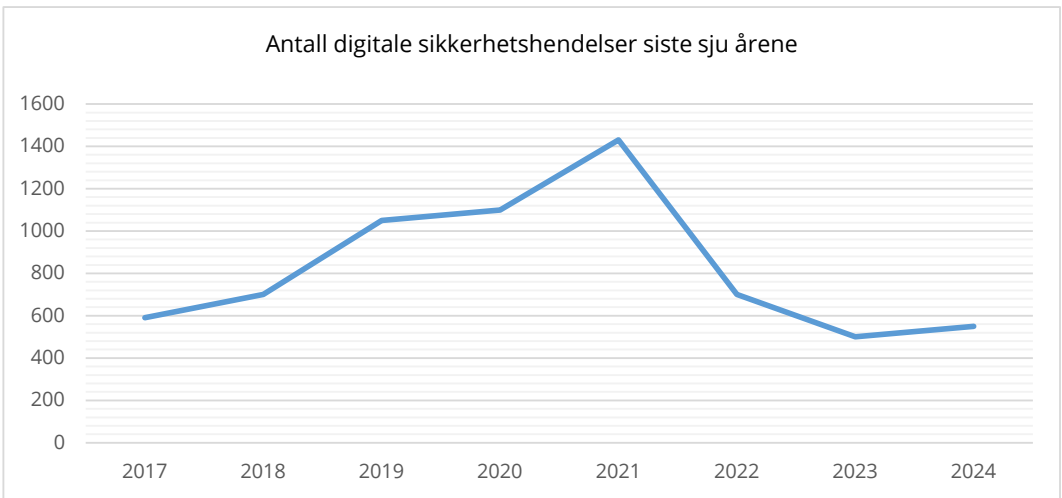


3.6 HENDELSER OG AVVIK VED NTNU I 2024

3.6.1 Digitale sikkerhetshendelser

En digital sikkerhetshendelse er en tilsiktet hendelse der områder eller enheter i NTNUs IKT-infrastruktur er under angrep eller står i fare for å bli angrepet. Hendelser eller mistanke om en hendelse rapporteres til operasjonssenteret i Seksjon for Digital sikkerhet (NTNU SOC) i IT-avdelingen for vurdering, koordinering og håndtering. Hendelser forekommer uavhengig av avvik, men mangel på etterlevelse av retningslinjer kan være en av flere grunner til at det forekommer hendelser.

I 2024 håndterte operasjonssenteret 550 sikkerhetshendelser hvor 7 (1%) av disse var regnet som alvorlig. Dette er en oppgang på 14 % fra 2023. De tre mest fram-tredende hendelsene som treffer NTNU er svindel (inkl. phishing), kompromitterte brukere og sårbare tjenester hvor det er en viss korrelasjon imellom antall saker på svindel og kompromitterte brukere, ofte i form av at mye phishing en måned, gir en økning i antall kompromitterte brukere måneden etter. Blant de 7 sakene vurdert som alvorlig, er det en sak som omhandler et målrettet forsøk på kompromittering i fra en statlig trusselaktør, dette var ikke vellykket.



Figur 9: Antall digitale sikkerhetshendelser siste sju årene.

KATEGORI	ANTALL
Svindel	300
Kompromittert bruker	117
Sårbare tjenester	72
Kompromittert enhet	46
Støtende innhold	9
Kompromittert informasjon	5
Forsøk på kompromittering	1
Annet	0
Totalt	550

Tabell 2: Kategorier av digitale sikkerhetshendelser i 2024.

3.6.2 Avvik informasjonssikkerhet og personvern

Et avvik er et brudd på en eller flere av retningslinjene innen informasjonssikkerhet og personvern. Et avvik er en viktig tilbakemelding på kvaliteten på NTNUs retningslinjer og om tiltak som er iverksatt i organisasjonen er tilstrekkelige. Ved NTNU meldes avvik innenfor informasjonssikkerhet og personvern inn i NTNUs avvikssystem. I tillegg meldes avvik oppdaget av Sikt personverntjenester inn i Sikt sin portal. Dette gjelder bare avdekkede avvik av Sikt i forsknings- og studentprosjekt som inneholder personopplysninger.

I 2024 er det registrert 98 avvik innen informasjonssikkerhet og personvern. Ni av avvikene er meldt til Datatilsynet. Hvis det skjer et brudd på personopplysningssikkerheten har NTNU som hovedregel plikt til å melde det til Datatilsynet innen 72 timer.

AVVIK KATEGORISERT ETTER ALVORLIGHETSGRAD	2023	2024
Innmeldt	72	98
Svært alvorlig	3	0
Alvorlig	20	24
Mindre alvorlig	35	58
Ikke vurdert	4	4
Avvist	8	9
Meldt til Datatilsynet	1	9

KATEGORIER AVVIK * Ett avvik kan kategoriseres innenfor flere av kategoriene	2023	2024
Personopplysninger i forskningsprosjekt (Sikt)	3	14
Personopplysninger	27	32
Brudd på konfidensialitet	29	35
Brudd på interne bestemmelser	10	0
Brudd på lover og regler	9	4
Brudd på tilgjengelighet	1	11
Manglende opplæring	5	4
Uautoriserte tilganger	3	0
Brudd på integritet	1	11
Manglende/Mangelfulle rutiner	13	27
Tap av data	0	3
Annet	2	4

Tabell 3: Avvik kategorisert etter alvorlighetsgrad

Det ble meldt inn 26 flere avvik innen informasjonssikkerhet og personvern i 2024 sammenlignet med 2023. I 2024 er det gjennomført mye arbeid innen opplæring og sikkerhetskultur som kan forklare oppgangen i innmeldte avvik. De reelle tallene for antall avvik innen informasjonssikkerhet og personvern er nok mye høyere enn det som vises i statistikken her. Arbeidet med opplæring og sikkerhetskultur fortsetter derfor i 2025.

3.6.3 HMS-avvik

NTNUs retningslinje for å melde avvik, uønskede hendelser og forbedringsforslag beskriver NTNUs retningslinjer for rapportering av HMS-avvik. NTNUs HMS-seksjon ivaretar oppfølging av avvik i denne kategorien. For mer informasjon om HMS-avvik i 2024 vises det til NTNUs årsrapport for HMS.

3.6.4 Sikkerhetstruende hendelser

Det er ikke etablert rutiner for varsling av sikkerhetsbrudd eller sikkerhetstruende hendelser ved NTNU i 2024. Manglende rutiner på dette gjør at NTNU har utilstrekkelig innsikt i faktiske hendelser og avvik på dette området. Seksjon for sikkerhet og beredskap har begynt arbeidet med å etablere rutiner for avviksregistrering og avvikshåndtering også på dette området. Arbeidet vil ha prioritet i 2025.

3.7 SIKKERHETSMYNDIGHETENES RISIKO- OG TRUSSELVURDERINGER

Årets trussel- og risikovurderinger fra [Etterretningstjenesten](#), [Politiets sikkerhetstjeneste](#) og [Nasjonal sikkerhetsmyndighet](#) ble presentert den 5.februar. Den geopolitiske situasjonen med krig i Ukraina og stormaktsrivalisering mellom Kina og vesten preger trussel- og risikobildet både i verdensbildet, nasjonalt og for UH-sektoren. De mest markante trusselaktører i Norge og som utgjør en trussel mot våre verdier er Russland og Kina. Samtidig finnes det andre aktører som Nord Korea og Iran. En markant endring fra tidligere års vurderinger er at det i år er sannsynlig at sabotasje vil forekomme i Norge.

Trusselaktørene er utfordrende å forholde seg til da de stadig utvikler sine virkemidler og verktøy for å lykkes i å nå våre verdier. Dette spesielt med bakgrunn i den teknologiske utviklingen. Ved NTNU er det særskilt etterretningstrusselen som utgjør et risikomoment. Samtidig må NTNU være bevisst på at man har et moderat terrortrusselnivå og at det er vurdert til at sabotasje er sannsynlig i 2025.

«Forskningsinstitusjoner og andre kunnskapsbedrifter vil i 2025 være særlig utsatte mål for tilnærmelser fra disse statlige aktørene. Disse vil blant annet forsøke å få tilgang til ansattes fasiliteter, slik som laboratorier og instrumenter, og vitenskap eller nettverk. De vil også bruke forskningssamarbeid, internasjonale konferanser og andre møtearenaer for å sikre seg tilgang til sensitiv teknologi eller skjermingsverdig informasjon.»

[PST NTV 2025 \(PDF-fil\)](#)



4. ANBEFALTE PRIORITERINGER FOR 2025

Det har skjedd mye viktig og godt arbeid innenfor sikkerhetsområdene ved NTNU i 2024. Mange av aktivitetene og tiltakene som er igangsatt i 2024 vil løpe videre inn i 2025, og en rekke nye behov er identifisert.

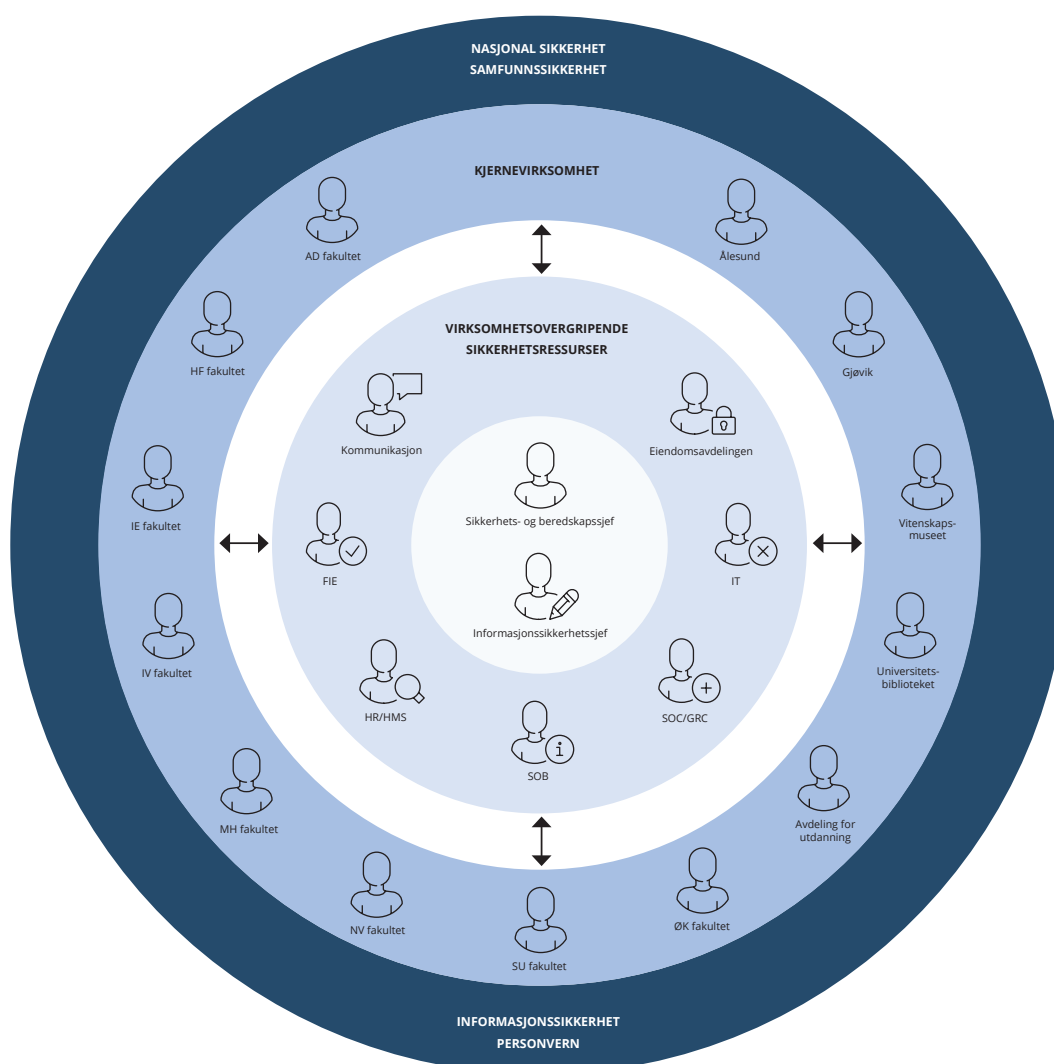


4.1 PRIORITERINGER INNEN NASJONAL SIKKERHET

4.1.1 Iverksetting av sikkerhetsorganisasjonen

De formelle rammene for sikkerhetsorganisasjonen er satt gjennom NTNUs styringsdokument for sikkerhet og beredskap. Dette definerer sikkerhetsorganisasjonen, men et stort og viktig arbeid med å iverksette sikkerhetsorganisasjonen gjenstår.

I 2025 vil de første møtearenaene for sikkerhetsorganisasjonen finne sted. Prioriteringer i første fase er etableringen av et felles begrepsapparat, og felles situasjonsforståelse for ansatte ved NTNU med en rolle i sikkerhetsorganisasjonen. Et første møte for sikkerhetsorganisasjonen i tilknytning til Sikkerhetsdagen ved NTNU i april er under planlegging.



4.1.2 Plan for revidering av eksisterende retningslinjer og rutiner

Styringsdokumentet for sikkerhet og beredskap skal følges opp med reviderte og oppdaterte retningslinjer og rutiner for sikkerhetsarbeidet. Sikkerhets- og beredskapssjef er ansvarlig for at det utvikles en plan for revidering av eksisterende retningslinjer og rutiner, og at eventuelle nye behov dekkes. Informasjonssikkerhetssjef er delegert ansvar for de områdene som berører informasjonssikkerhet. Det er blant annet behov for å revidere Politikk for sikkerhet og beredskap, for å sikre et helhetlig og oppdatert styringssystem. Revisjon av styringssystem for informasjonssikkerhet og personvern (ISMS) har et revisjonsintervall på to år. IKT-reglementet, Politikk for informasjonssikkerhet samt alle retningslinjer tilknyttet ISMS må gjennomgås og oppdateres. Revisjonen av ISMS startet i januar 2025. Forslag til reviderte dokumenter vil bli sendt på høring i organisasjonen i april/mai 2025.

4.1.3 Årlig trusselvurdering

Fra 2025 vil NTNU utarbeide en årlig sammenfatning av de nasjonale trusselvurderingene for NTNU. Sammenfatningen for 2025 ble utarbeidet i februar og delt med utnevnte sikkerhetsressurser ved enhetene, like etter offentliggjøringen av trusselvurderingene fra de nasjonale sikkerhetsmyndighetene. Hensikten er å gi NTNUs ledelse og sikkerhetsorganisasjonen en grundig sammenstilling av de nasjonale trusselvurderingenes betydning for NTNU og kunnskapssektoren. Informasjonspakken utarbeides av Seksjon for sikkerhet og beredskap i samarbeid med et utvalg sikkerhetsressurser ved fakultetene. Informasjonspakken har til hensikt å holde NTNUs lederlinje godt informert om trusselvurderingene, samt å bistå lederlinjen i gjennomføring av vurderinger på lokalt nivå om hva trusselbildet betyr for enheten. På denne måten understøttes enhetenes forebyggende arbeid med sikkerhetsstyring.

4.1.4 Verdikartlegging

NTNU skal ha oversikt over verdier og avhengigheter med hensyn til nasjonal sikkerhet. Som vist i første del av årsrapporten ble det gjennomført en pilot innen verdikartlegging i 2024, men det ikke enda utviklet en felles metodikk eller lagt opp interne prosesser for verdikartlegging i organisasjonen. I henhold til ROS SOB24 må det etableres en metodikk og prosess for å få oversikt over verdier, og vurdere deres beskyttelsesbehov med utgangspunkt i verdienes betydning, gjeldende lovverk og trusselbilde. Slik vurdering må skje lokalt, og inngå i sikkerhetsstyringen. Gjennomføring av verdikartlegging opp imot nasjonal sikkerhet er også et tydelig krav til NTNU gjennom NTNUs årlige tildelingsbrev fra KD.

Et arbeid med å utrede behov knyttet til verdikartlegging med hensyn til nasjonal sikkerhet vil iverksettes i løpet av våren 2025, med målsetning om å forankre metodikk og prosess for verdivurdering som del av sikkerhetsstyringen.

4.1.5 Sikkerhetstruende hendelser

Det har ikke etablert rutiner for rapportering av sikkerhetsbrudd eller sikkerhetstruende hendelser ved NTNU. Manglende rutiner på dette gjør at NTNU har utilstrekkelig innsikt i faktiske hendelser og avvik på dette området. Seksjon for sikkerhet og beredskap har begynt arbeidet med å etablere rutiner for avviksregistrering og avvikshåndtering også på dette området. Arbeidet vil ha prioritet i 2025.

4.1.6 Etablere en kompetanse- og opplæringsplan

Systematisk arbeid med sikkerhetskultur er viktig. Kunnskap, holdninger, og kompetanse har stor betydning for evne til sikkerhetsstyring og risikovurdering. Ledere, ansatte og studenter skal være i stand til å ivareta sikkerhet i sin egen arbeids- og studiehverdag.

Internrevisjonen i 2023 anbefalte at NTNU bør etablere en kompetanse- og opplæringsplan, som spesifiserer hvilke ansatte/gjester/studenter som har behov for en grunnforståelse for sikkerhet og eksportkontroll, og hvilke som har behov for mer inngående kunnskap. KD anbefaler at Sikresiden.no innlemmes i universitetenes informasjons- og opplæringsarbeid. Ved etablering av en kompetanse- og opplæringsplan innen sikkerhet vil det være naturlig å vurdere hensiktsmessig integrering av ressurser utviklet av Sikresiden.no, som er utviklet av og for UH-sektoren.

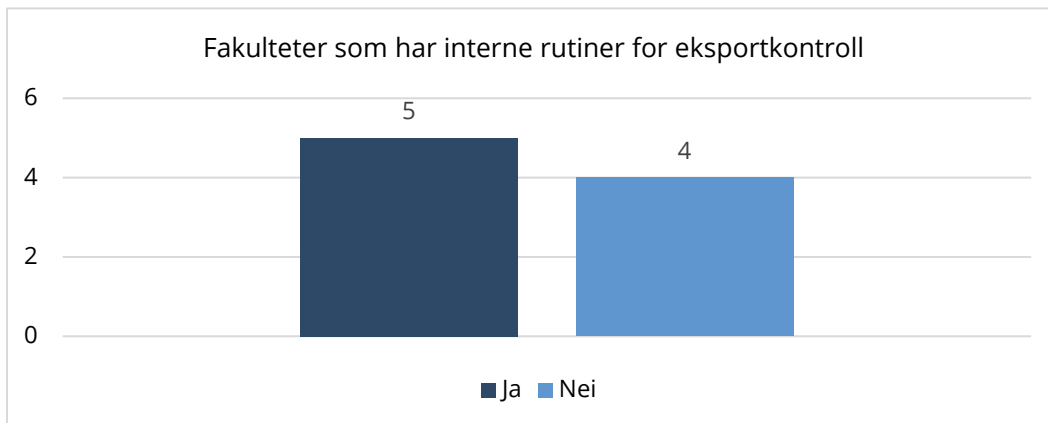
4.1.7 Personellsikkerhet

[Sikkerhetsloven](#) og [Virksomhetssikkerhetsforskriften](#) stiller krav til hvordan virksomheter skal forvalte personellsikkerhet. For å gjøre NTNU og sikkerhetsressurser i stand til å utøve dette, prioriteres etablering av intern opplæring, samt utvikling av god praksis. Dette er spesielt relevant for NTNUs samarbeid med Forsvaret, og for NTNUs deltakelse i graderte European Defence Fund (EDF) prosjekter. Seksjon for sikkerhet og beredskap vil i løpet av 2025 etablere intern opplæring i tråd med retningslinje for personellsikkerhet ved NTNU, samt gjennom etablering av et mindre nettverk, etablere gode rutiner og praksis knyttet til forvaltningen av området.

4.1.8 Eksportkontroll

HK-dir anbefaler at eksportkontroll inngår som del av virksomhetens helhetlige risikostyring. NTNU har dedikerte sikkerhetsressurser ved de teknologiske fakultetene som ivaretar lokalt arbeid med eksportkontroll. Disse ressursene deltar i NTNUs eksportkontrollklynge, og samarbeider med nivå 1 som har fagansvar innen eksportkontroll i Fellesadministrasjonen.

Årsrapportering viser at flertallet av fakultetene har interne rutiner for eksportkontroll. HK-dir anbefaler jevnlig oppdatering, bevisstgjøring og kjennskap til interne rutiner for å sikre god etterlevelse av eksportkontrollregelverket. Seksjon for sikkerhet og beredskap vurderer at en gjennomgang av NTNUs rutiner for eksportkontroll i løpet av 2025 synes nødvendig. Målsetningen for et slikt arbeid vil være kvalitetssikring av rutinene, og sikre standardiserte, gjennomgående prosesser. En gjennomgang av rutinene er også relevant med bakgrunn i etableringen av det nye direktoratet for eksportkontroll og sanksjoner; DEKSA.



Figur 10: Fakulteter som har interne rutiner for eksportkontroll. Kilde: Årsrapportering 2024

4.2 PRIORITERINGER INNEN SAMFUNNSSIKKERHET

4.2.1 Revisjon av NTNUs krise- og beredskapsplanverk

[Kunnskapsdepartementet](#) stiller krav om at virksomhetene utarbeider og vedlikeholder krise- og beredskapsplaner for å håndtere uønskede hendelser, og at planverket utarbeides på grunnlag av virksomhetens ROS-analyse.

Det er viktig at NTNU til enhver tid sørger for at beredskapsplanverket er oppdatert. Som del av NOKUTS kontroll av NTNUs arbeid med samfunnssikkerhet i 2024 er detpekt på behovet for å revidere krise- og beredskapsplanverket til NTNU i tråd med ROS SoB24, samt å utarbeidelse av en beredskapsplan for opprettholdelse av kritiske funksjoner ved høyt personellfravær, uavhengig av årsak (kontinuitetsplan). Dette arbeidet vil prioriteres i 2025.

4.2.2 Krise- og beredskapsøvelse

Øving er en viktig læringsarena for å lykkes med krisehåndtering. Det vil utarbeides en årlig, overordnet øvelsesplan for krise- og beredskaps øvelser ved NTNU. Øvingsplanen skal bidra til systematisk tilnærming til øving. Ved prioritering av øvingsscenario vil ROS SOB24 anvendes som utgangspunkt, med fokus på uønskede hendelser med høy eller middels risiko.

4.2.3 Opplæring og kompetanseheving

Seksjon for sikkerhet og beredskap bistår enheter og fakulteter med kompetanseheving knyttet til beredskap og krisehåndtering. Seksjonen vil fortsette dette arbeidet i 2025.

I forbindelse med etableringen av ny temaside og nye wikisider for sikkerhet og beredskap, skal vi som en del av dette arbeidet jobbe med å utvikle og samle relevant opplæringsmateriell og kompetansehevende tiltak på ny wikiside til bruk for alle enheter og fakulteter.

4.3 PRIORITERINGER INNEN INFORMASJONSSIKKERHET

4.3.1 Revisjon av styringssystem for informasjonssikkerhet og personvern

Revisjon av styringssystem for informasjonssikkerhet og personvern (ISMS) har et revisjonsintervall på to år. Siste revisjon ble utført i 2023. Siden sist revisjon har det skjedd endringer både på NTNU og i lovverk, som gjør at deler av styringssystemet er utdatert og nye elementer må legges til.

Tiltaket innebærer at IKT-reglementet, politikk for informasjonssikkerhet samt alle retningslinjer tilknyttet ISMS må gjennomgå og oppdateres. I tillegg til å korrigere dokumentene i ISMS til nå-situasjonen vil de bli gjennomgått for å sikre mer klar-språk. Revisjonen av ISMS startet i januar 2025 og forslag til reviderte dokumenter vil bli sendt ut på høring i organisasjonen i april/mai 2025.

4.3.2 Grunnsikring av digital infrastruktur

Arbeidet med grunnsikring av digital infrastruktur fortsetter i 2025. Arbeidet er tid- og ressurskrevende, og fører til driftsbrudd. Gjennomføring av arbeidet i en takt som organisasjonen klarer å håndtere er derfor avgjørende. I 2025 fortsetter arbeidet med:

- Nettverk og sonemodell; som inkluderer å begrense trafikkflyt i brannmur og gradvis flytte tjenester, klienter og laboratoriestyr inn i den nye sikkerhets- og sonemodellen.
- Innskjerpning av privilegert tilgangskontroll i NTNUs systemer; som også innebærer å begrense lokal administrator på klientmaskiner, skyplattformer og liknende.
- Revurdere enterpriseavtale på sikkerhetsløsninger og eventuelt bytte leverandør / løsning.

4.3.3 Økt bevissthet om behovet for informasjonssikkerhet

Opplæring innen informasjonssikkerhet er avgjørende for å skape økt bevissthet i organisasjonen i møte med et økende antall cybertrusler. Det er behov for å øke formidlingsinnsatsen ut i organisasjonen om betydningen av informasjonssikkerhet. Derfor iverksettes flere tiltak:

- Wikisider om informasjonssikkerhet ved NTNU skal revideres og oppdateres med relevante eksempler.
- Seksjon for digital sikkerhet vil ha økt fokus på formidling på Innsida og andre interne kanaler, med publisering av artikler som tar utgangspunkt i reelle digitale sikkerhetshendelser og avvik, for å aktualisere innholdet for ansatte og studenter.
- NTNUs obligatoriske opplæring i informasjonssikkerhet bli videreutviklet. Det skal også utvikles opplæring for sentrale roller i organisasjonen.

Bevisstgjøring og opplæring er et kontinuerlig arbeid. Et utviklingsarbeid knyttet til opplæring for ansatte i sentrale roller forberedes til høsten 2025, da mange ledere ved NTNU starter sine åremål.

4.4 PRIORITERINGER INNEN PERSONVERN

Det er vedtatt en handlingsplan for fagområdet personvern for å redusere identifisert etterslep. Planen operasjonaliseres for å sikre etterlevelse av regelverk, kontinuerlig kvalitetsforbedring, og sikre en robust organisering av personvernarbeidet ved NTNU. Handlingsplanen er delt opp i seks områder som utgjør fundamentet for NTNUs etterlevelse av personvernfeltet, og sikrer at NTNU forvalter personopplysninger på en trygg og ansvarlig måte.

Handlingsplanen er utarbeidet på bakgrunn av gjennomført kartlegging i 2024 av anbefalinger fra gjennomførte revisjoner, og adresserer nødvendig oppfølgingsarbeid.

De seks områdene innebærer en rekke oppgaver og mål, med hensikt om å sikre fremdrift og etterlevelse:

- **Rammeverk:** Etablere en robust organisering av fagansvar for personvern på NTNU som skal sikre etterlevelse av regelverk, kontinuerlig og systematisk kvalitetsforbedring, og at NTNUs organisering tåler interne og eksterne endringer.
- **Protokoll:** Etablere og opprettholde en oppdatert oversikt over all behandling av personopplysninger, inkludert i administrative saksprosesser, systemer, og i student- og forskningsprosjekt.
- **Informasjon til de registrerte:** Sørge for at informasjon som gis til de registrerte via NTNUs nettsider, personvernerklæringer og retningslinjer for behandling av personopplysninger er være lett tilgjengelig, forståelig, åpen og tilpasset mottakeren.
- **Prosedyrer:** Implementere standardiserte prosedyrer og retningslinjer for håndtering av personopplysninger for å sikre helhetlig behandling av personopplysninger i hele organisasjonen.
- **Opplæring:** Utvikle en helhetlig opplæringsplan for personvern som sikrer at alle relevante aktører har nødvendig kompetanse og forståelse for å gjennomføre sine oppgaver i henhold til gjeldende regelverk.
- **Avvikshåndtering:** Etablere en robust og effektiv avvikshåndtering, som kontinuerlig forbedrer sikkerhetsnivået og sikringstiltak gjennom systematisk evaluering og læring etter avvik fra rutiner, hendelser og brudd på personopplysningssikkerheten, samt gjennomføre årlig internkontroll av innmeldte avvik for å sikre kontinuerlig og systematisk kvalitetsforbedring.

