Retningslinje for Digital beredskap, hendelse- og krisehåndtering

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	ISO/IEC 27002:2022 5.5-5.7, 5.24, 5.25, 5.27, 5.29, 5.30, 6.4, 6.8, ISO/IEC 27035-2:2016 4.3b, 4.6e
Referanse NSMs Grunnprinsipper for IKT-sikkerhet	1.3.3b,3.3.1-3.3.7, 3.4.1-3.4.6, 4.1.1-4.1.6, 4.2.1-4.2.3, 4.3, 4.4
Referanse LOV/Regel	
Referanse interne dokumenter	Politikk for informasjonssikkerhet, Politikk for sikkerhet og beredskap, Retningslinje for klassifisering av informasjon

1. Formål

Formålet med denne retningslinjen er å stille krav til kvalitet innen digital beredskap, digital krisehåndtering og håndtering av sikkerhet og driftshendelser. Retningslinjen definerer roller og ansvar for arbeidet med hendelseshåndtering for NTNU.

2. Gjelder for

"Retningslinje for Digital beredskap, hendelses- og krisehåndtering" gjelder for alle som benytter, forvalter og drifter IKT-systemer på NTNU, men med særskilt vekt på:

a. IT-ansatte ved NTNU
b. Systemeiere
c. Linjeledere

3. Overordnede prinsipper

a. Sikkerhetshendelser skal rapporteres til, håndteres, og koordineres av NTNU SOC ved Seksjon for Digital sikkerhet.
b. Seksjon for Digital sikkerhet skal kunne utføre sitt arbeid uhindret.
c. NTNU skal følge ansvarsprinsippet, likhetsprinsippet, nærhetsprinsippet og samvirkeprinsippet i arbeidet med hendelseshåndtering og digital beredskap
d. Planverk for digital hendelseshåndtering skal bygges på ITIL, ISO27035 og NSMs Rammeverk for håndtering av IKT-hendelser
e. NTNU skal ha rutine for sikring og håndtering av data og bevismateriale.
f. NTNU skal ha rutine for deling av informasjon og data om hendelser.
g. NTNU skal ha rutine for trening, evaluering og forbedring av beredskapsplaner.

4. Hendelseshåndtering

En sikkerhetshendelse er en hendelse med bakgrunn i et tilsiktet brudd, eller en nært forestående trussel om et tilsiktet brudd på konfidensialitet, integritet eller tilgjengeligheten i et system, tjeneste, applikasjon eller informasjon/data, eller et brudd på IKT-reglementet, politikk for informasjonssikkerhet med retningslinjer eller gjeldende sikkerhetspraksis.

a. Plan for hendelseshåndtering skal være et sett med rutiner og prosedyrer som skal utføres før, under og etter at en hendelse har oppstått. En hendelse er et ikke-planlagt brudd eller reduksjon av kvalitet på en tjeneste som er i produksjon, eller en hendelse som i fremtiden kan føre til reduksjon av kvalitet eller brudd på en tjeneste.
b. Plan for hendelseshåndtering skal definere prosedyrer for å identifisere, klassifisere, håndtere og gjenopprette normal drift ved hendelser.
c. Plan for hendelseshåndtering med rutiner, prosedyrer og verktøy er underlagt taushetsplikt for å beskytte den operasjonelle sikkerheten til funksjonen hendelse og krisehåndtering.

4.1 Organisering av hendelseshåndtering

a. NTNU Security Operations Centre (SOC) har det operative ansvaret for å detektere trusler, koordinere, håndtere og analysere sikkerhetshendelser på NTNUs digitale infrastruktur.
b. IT Incident Manager (IM) har det operative ansvaret for å håndtere og koordinere hendelser relatert til tjenestekvalitet av IKT tjenester ved NTNU. IM er prosesseier for ITIL prosessen «Incident Management» som har i oppgave, og som mål, å gjenopprette normal tjenesteleveranse så raskt som mulig for å minimalisere negativ effekt for virksomheten og brukere når en tjeneste er utilgjengelig eller redusert.
c. NTNU CSIRT er en utvidet teknisk sikkerhetsgruppe og en støtteressurs for NTNU SOC som arbeider med forebyggende digital sikkerhet innenfor sitt fagområde og hendelseshåndtering

4.2 Rapportering av hendelser og sårbarheter

a. Hendelser som er et sikkerhetsbrudd eller som kan mistenkes å være sikkerhetsbrudd skal rapporteres til NTNU SOC[1] ved Seksjon for Digital sikkerhet uten unødvendig opphold.
b. Sårbarheter eller mistanke om en sårbarhet skal rapporteres til NTNU SOC ved Seksjon for digital sikkerhet for vurdering.
c. En driftshendelse ved NTNU er en hendelse som kan kategoriseres etter tabell i 4.3.4.
d. Driftshendelser skal rapporteres til Incident Manager.

4.3 Vurdering av hendelser og sårbarheter

a. Hendelser skal være kategorisert, prioritert og tildelt innen 30 minutter i vanlig arbeidstid (08:00-15:45 / 08:00-15:00 Sommertid)
b. Hendelser skal kategoriseres etter tabell i 4.3.1
c. Hendelser prioriteres etter klassifisering av system og informasjon iht. «Retningslinje for klassifisering av informasjon»
d. Triage prosedyre skal prioritere hendelser basert på klassifisering og etter hendelsens:

[1] https://www.ntnu.no/adm/it/ntnu-soc

- grad av negativ innvirkning på funksjonaliteten til et system, applikasjon eller tjeneste (Functional Impact)
- grad av negativ innvirkning på konfidensialiteten og integriteten i relasjon til informasjon (Information Impact)
- grad av negativ innvirkning på muligheten til å gjenopprette normal drift av tjenesten eller systemet innen en gitt tid (Recoverability Impact).

4.3.1 Kategorisering av sikkerhetshendelser

NTNU	NSM	Beskrivelse / Eksempler
Støtende innhold (Abusive content)	Støtende Innhold	Spam og uønsket epost, publisering av innhold som strider imot etiske retningslinjer, trusler og forfølgelse via digitale kanaler, distribusjon av ulovlig materiale via NTNUs ressurser.
Informasjonsinnsamling (Information gathering)	Rekognosering / Informasjonssamling	Informasjonsinnhenting, nettverksskanning, sårbarhetsskanning og sosial manipulasjon.
Forsøk på kompromittering (Intrusion attempts)	Forsøk på Kompromittering	Forsøk på kompromittering av systemer eller tjenester ved å utnytte sårbarheter i system/tjeneste eller feilkonfigurasjon, gjette passord eller forsøk på å omgå sikkerhetsmekanismer, forsøk på skadevareinfeksjon.
Kompromittert ressurs (Compromised asset)	Kompromittering	Vellykket uautorisert privilegert tilgang til system eller tjeneste, tap/tyveri av utstyr og enheter, vellykket skadevare infeksjon.
Kompromittert bruker (Compromised user)	Kompromittering	Vellykket uautorisert tilgang til en brukerkonto, lekkasje av brukerkontoer med passord.
Kompromittert informasjon (Compromised information)	Kompromittering	Vellykket uautorisert tilgang til data eller informasjon, lekkasje av informasjon, Lekkasje av personopplysninger.
Sårbarhet (Vulnerability)	Rekognosering / Informasjonssamling	Sårbar, feilkonfigurert og eksponert applikasjon, tjeneste eller system
Tilgjengelighet (Availability)	Tjenestenekt	Tjenestenekt / Distribuert tjenestenekt angrep mot system, tjeneste eller applikasjon, sabotasje.
Svindel (Fraud)	Svindel	Phishing, Smishing, Telefonsvindel, Utpressing, Uautorisert bruk av NTNUs ressurser.
Annet (Other)	-	Hendelser som truer den digitale sikkerheten til NTNU, men som ikke kan kategoriseres i de andre kategoriene.

4.3.2 Kategorisering av driftshendelser

a. Tabellen viser hovedkategorier av IKT driftshendelser definert ved NTNU. Dersom det er hensiktsmessig med finere granulering, kan underkategorier benyttes. Underkategorier defineres i plan for hendelseshåndtering.

Kategori	Definisjon

Maskinvarefeil	Fysisk feil på maskinvare, inkludert fastvare
Programvarefeil	Logisk feil i programvare
Konnektivitetsfeil	Fysisk eller logisk feil på nettverksutstyr
Driftsmiljøfeil	Fysisk feil på driftsmiljø der IKT-infrastruktur er plassert
Rutinefeil	Menneskelig feil, inkludert feilhåndtering, dårlig konfigurasjonsstyring etc.
Brukerfeil	Menneskelig feil.

4.3.3 Responstid

a. Responstid er den maksimale tiden i fra en hendelse oppstår/rapporteres til arbeidet med hendelse eller krisehåndtering begynner innenfor normal arbeidstid.
b. Nedetid er akseptabel nedetid for systemet/utilgjengelighet for informasjonen

Klassifisering	Responstid	Akseptabel nedetid
Virksomhetskritisk	30 min	Ingen
Funksjonskritisk	60 min	4 timer
Alvorlig	4 t	2 dager
Mindre alvorlig	48 t	Over 2 dager

4.4 Deling av sikkerhetshendelser

NTNU skal etterleve den etablerte trafikklysprotokollen (TLP)[2] for deling av informasjon og data relatert til trusler og sikkerhetshendelser (tabellen under) for å kunne motta, dele, koordinere og samhandle med UH-sektor og internasjonale, nasjonale, og private responsmiljøer. TLP var utviklet for å kunne fasilitere deling av informasjon relatert til sikkerhetshendelser. TLP er et sett med retningslinjer (fargekoder) som blir brukt til å merke informasjon for å sikre at den sensitive informasjonen blir delt på en forsvarlig måte.

Trafikklysprotokollen (TLP)	Anbefalt NTNU gradering	Beskrivelse	Forutsetning for deling
TLP:RED	Nivå 4 *Strengt Fortrolig / Unntatt Offentlighet Jfr. Offl. §24.3*	Informasjon er kun til mottaker. Hvis det er nødvendig å gi informasjonen videre må mottaker ha informasjonseiers godkjennelse for å gi det til en navngitt person.	Eier vil ha kontroll over navngitte personer som har informasjonen.
TLP:AMBER TLP:AMBER+STRICT	Nivå 3 *Fortrolig / Unntatt Offentlighet Jfr. Offl. §24.3*	Informasjon til mottakers virksomhet (inkl. konsulenter, outsourced personell som arbeider for virksomheten) som har en need to know og gyldig taushetserklæring for å gjøre de nødvendige tiltakene. Hvis mottaker ønsker å gi informasjonen til andre virksomheter, må de ha informasjonseiers godkjennelse for å gi det til en navngitt virksomhet.	Eier vil ha kontroll over navngitte virksomheter som har informasjonen.
TLP:GREEN	Nivå 2 *Intern / Unntatt*	Informasjonen kan deles med andre virksomheter eller personer innen informasjonssikkerhetsmiljøet, men	Eier vil ikke ha kontroll over spredningen, men forutsetter at ingen

[2] https://www.first.org/tlp/

	Offentlighet *Jfr. Offl. §24.3*	skal ikke publiseres eller legges ut på websider/åpne mailinglister.	mottaker publiserer informasjonen
TLP:CLEAR	Nivå 1 *Åpen*	Informasjonen er offentlig tilgjengelig, publiseres, og spres til publikum. Enhver kontaktperson kan publisere informasjonen.	Eier av informasjonen forventer at informasjonen offentliggjøres.

4.5 Tilgang, datainnsamling og bevissikring

a. Plan for hendelseshåndtering skal ha en rutine for datainnsamling og sikring av bevis med prosedyrer. Denne rutinen skal definere når datainnsamling skal finne sted og hvilken hjemmel som ligger til grunn for innsamlingen.
b. Prosedyrer for datainnsamling og sikring av bevis skal sørge for at:
    - datainnsamling kommer i gang så fort som mulig og utføres av kompetent personal
    - datainnsamling er i henhold til lover og regler
    - datainnsamling følger prinsippene for «Forensic Soundness»
    - datainnsamlingen følger prinsippet for «Order of volatility»
    - datainnsamlingen håndteres forsvarlig og korrekt
    - datainnsamlingen slettes/destrueres når behovet for behandling opphører
    - All data som samles inn lagres og prosesseres på en måte som ivaretar konfidensialitet, integritet og personvern.
c. NTNU SOC skal ha lesetilgang på data i fra alle systemer og tjenester for å kunne utføre sikkerhetsanalyse.
d. NTNU IRT skal ha tilgang som systemadministrator på alle systemer for å kunne håndtere hendelser.
e. Personer som skal håndtere datainnsamling og bevismateriale skal ha dokumentert kompetanse som viser at tilstrekkelig kunnskap til å utføre denne oppgaven er til stede. Dette skal være godkjent av Seksjon for digital sikkerhet.

4.6 Øvelse og revisjon av plan for hendelseshåndtering

a. Plan for hendelseshåndtering skal revideres minst en gang i året for å sikre relevans i henhold til det oppdaterte trussel- og risikobildet for NTNU. Dette arbeidet skal ta utgangspunkt i ROS-vurderinger, håndterte hendelser og trender innen trusselbildet.
b. Prosedyrer på hendelser skal dokumenteres og godkjennes for implementasjon i planen fortløpende dersom de ikke eksisterer i plan for hendelseshåndtering.
c. Prosedyrer under plan for hendelseshåndtering skal revideres fortløpende etter at de har vært benyttet som en del av rutine for post-hendelseshåndtering.
d. Plan for hendelseshåndtering skal minimum øves årlig.

5. Digital krisehåndtering

En krise er enhver hendelse, ventet eller uventet, som setter liv eller NTNUs kjernevirksomhet i fare, eller som reduserer NTNUs evne til å utføre normal drift[3]. En krise har klassifisering som enten virksomhetskritisk (K1) eller funksjonskritisk (K2).

[3] Politikk for beredskap ved NTNU

a. Plan for krisehåndtering bygger på prosedyrer for å håndtere krise hvor målet er å minimere konsekvens og gjenopprette normal drift så fort som mulig. Planen er også en utvidelse av plan for hendelseshåndtering som beskriver rutiner for forberedelse til håndtering av krise. Planen skal minimum inneholde:
    - prosedyre for effektiv mobilisering av roller og funksjoner slik at krisehåndtering kommer raskt i gang
    - prosedyre for kommunikasjon og samhandling mellom relevante parter
    - prosedyre for å eskalere og aktivere sentral beredskapsledelse for virksomheten
    - prosedyre for aktivering av plan for virksomhetskontinuitet
    - prosedyre for å innhente, prosessere, bearbeide og anvende informasjon for å bygge et situasjonsbilde som gir et best mulig beslutningsgrunnlag
b. Plan for krisehåndtering skal minimum dekke funksjonskritiske og virksomhetskritiske tjenester og systemer. Dette er kriser som påvirker undervisning, forskning, formidling, nyskapning samt administrasjon og forvaltning.
c. Plan for krisehåndtering skal identifisere ressursbehov for å kunne gjenopprette normal drift i fra en krise.
d. Plan for krisehåndtering skal ha en risikobasert tilnærming og basere seg på risiko- og sårbarhetsanalyse med en analyse av virksomhetskritiske effekter (Business Impact Analysis).

5.1 Organisering av krisehåndtering

a. Ansvar og roller i plan for krisehåndtering skal bestå av relevante funksjoner som har kompetent personell og ressurser til å håndtere en krise. Organisering av krisehåndtering skal defineres etter:
    - ansvarsprinsippet som betyr at den som har et ansvar i en normalsituasjon også har dette ansvaret i tilfelle ekstraordinære hendelser
    - likhetsprinsippet som betyr at den organisasjonen som skal håndtere en krise, er mest mulig lik den daglige organisasjonen
    - nærhetsprinsippet som betyr at kriser skal håndteres på lavest mulig nivå
    - samvirkeprinsippet som innebærer initiativ til at krisehåndteringen samordnes og koordineres mellom de involverte.

5.2 Øvelse og revisjon av plan for krisehåndtering

a. Plan for krisehåndtering skal revideres periodisk for å sikre at den er oppdatert og dekker kritiske virksomhetsfunksjoner.
b. Plan for krisehåndtering skal testes jevnlig og minimum en gang i året. Læringsutbyttet skal benyttes til å kvalitetssikre, videreutvikle og forbedre planverket og rollene som inngår i organisasjon for krisehåndtering slik at ledelse og ansatte forstår gjennomføringen.
c. Plan for krisehåndtering skal basere seg på en risikobasert tilnærming hvor risiko- og sårbarhetsanalyse og analyse av virksomhetseffekt (BIA) ligger til grunn for planen.

5.3 Virksomhetskontinuitet

Planlegging av virksomhetskontinuitet betyr å etablere risikostyringsprosesser og prosedyrer som tar sikte på å forhindre forstyrrelser i virksomhetskritiske tjenester, og å gjenopprette full funksjon til organisasjonen så raskt og jevnt som mulig.

a. Plan for virksomhetskontinuitet bygger på plan for krisehåndtering, og er en utvidelse av denne.

b. Plan for virksomhetskontinuitet skal bestå av rutiner og prosedyrer for å ivareta drift av eller gjenopprettelse av virksomhetskritiske tjenester (T4) frem til normal drift kan gjenopprettes.
c. Plan for virksomhetskontinuitet skal sørge for teknisk støtte til sentral beredskapsgruppe for å kunne utføre oppgaven ved bortfall av nødvendig infrastruktur.
d. Plan for virksomhetskontinuitet skal dokumentere minimum ressursbehov for å kunne aktiveres, og ressursbehov for å kunne være aktiv.
e. Plan for virksomhetskontinuitet skal minimum ha prosedyre for å
    - flytte eller gjenopprette teknisk infrastruktur og funksjoner for beredskapsstøtte
    - flytte eller gjenopprette drift av virksomhetskritiske tjenester på midlertidige lokasjoner
    - flytte IT-avdelingen til midlertidig lokasjon for å ivareta drift av virksomhetskritiske tjenester eller gjenopprette drift av virksomhetskritiske tjenester
    - flytte tilbake i lokaler og gjenopprette normal drift etter en krise

6. Roller og ansvar

6.1 Direktør for Organisasjon og infrastruktur

a. er delegert myndighet som øverste beredskapsansvarlig ved NTNU
b. er lokal beredskapsansvarlig for fellesadministrasjonen

6.2 Leder av IT-avdelingen

a. er beredskapsansvarlig for IT-avdelingen
b. er ansvarlig for hendelse og krisehåndtering i IT-avdelingen
c. godkjenner plan for hendelseshåndtering
d. godkjenner plan for krisehåndtering

6.3 Leder av HR- og HMS-avdelingen

a. godkjenner plan for virksomhetskontinuitet
b. skal påse at nødvendige ressurser er tilgjengelig og disponibelt i NTNU IRT
c. er ansvarlig for at ledere er kjent med, og har tilstrekkelig kompetanse, til å ivareta sitt ansvar i henhold til denne retningslinjen

6.4 Leder av Kommunikasjonsavdelingen

a. skal påse at nødvendige ressurser er tilgjengelig og disponibelt i NTNU IRT

6.5 Leder av Avdeling for virksomhetsstyring

a. skal påse at nødvendige ressurser er tilgjengelig og disponibelt i NTNU IRT

6.6 Leder av Seksjon for digital sikkerhet

a. er ansvarlig for å implementere plan for hendelseshåndtering
b. er ansvarlig for å implementere plan for krisehåndtering
c. er ansvarlig for å detektere, koordinere og håndtere sikkerhetshendelser
d. er ansvarlig for å detektere, koordinere og håndtere sårbarheter
e. er ansvarlig for prosedyre for triage av sikkerhetshendelser
f. er ansvarlig for NTNU IRT
g. skal påse at plan for hendelseshåndtering følges i seksjon for digital sikkerhet

6.7 Leder av Seksjon for IT-drift

a. er beredskapsleder for IT-avdelingen
b. er ansvarlig for å detektere, koordinere og håndtere driftshendelser
c. er ansvarlig for klassifisering av driftshendelser
d. er ansvarlig for prosedyre for triage av driftshendelser
e. skal påse at nødvendige ressurser er tilgjengelig og disponibelt i NTNU IRT
f. skal konsulteres angående plan for hendelseshåndtering
g. skal konsulteres angående plan for krisehåndtering
h. skal påse at plan for hendelseshåndtering følges i seksjon for IT-drift

6.8 Leder av seksjon for IT-utvikling

a. skal informeres om endringer i retningslinje for hendelse og krisehåndtering
b. skal påse at nødvendige ressurser er tilgjengelig og disponibelt i NTNU IRT
c. skal påse at plan for hendelseshåndtering følges i seksjon for IT-utvikling

6.9 Leder av Seksjon for IT-brukerstøtte

a. skal informeres om endringer i retningslinje for hendelse og krisehåndtering
b. skal påse at plan for hendelseshåndtering følges i seksjon for IT-brukerstøtte