

Rutine ved utlevering av elektronisk lagret materiale til politi eller påtalemyndighet

Innhold

1. Innledning	2
1.1. Mål	2
1.2. Gyldighetsområde	2
1.3. Forhold til andre sikkerhetsdokumenter.....	2
2. Definisjoner.....	2
3. Rutiner.....	2
3.1. Prinsipper	2
3.2. Parter	2
3.3. Skriftlig henvendelse.....	3
3.4. Muntlig henvendelse	3
3.5. Rutine for tilbakemelding	3
3.6. Utlevering av driftslogger	3
3.6.1. Identifisering av bruker fra driftslogger	3
3.6.2. Utlevering av andre driftslogger	3
3.7. Utlevering av filer og e-post.	4
3.7.1. Sikring av materiale etter begjæring fra politi/påtalemyndighet.....	4
3.7.2. Utlevering.....	4
3.7.3. Forholdet til brukeren.....	4
3.8. Dokumentasjon, arkivering	4
3.8.1. Dokumentasjon av saksgang	4
3.8.2. Arkivering	4
3.8.3. Offentlighet	5
4. Ansvarlig for dokumentet	5
5. Revisjoner og endringer	5
6. Referanser, lenker	Feil! Bokmerke er ikke definert.

PostadresseHøgskoleringen 1
7491 Trondheim**Org.nr.** 974 767 880

E-post:

<http://www.ntnu.no/administrasjon>**Besøksadresse**Hovedbygget
Gløshaugen**Telefon**

+ 47 73 59 50 00

Telefaks

+ 47 73 59 80 99

Tlf: + 47

All korrespondanse som inngår i saksbehandling skal adresseres til saksbehandleren ved NTNU og ikke direkte til enkeltpersoner. Ved henvendelse vennligst oppgi referanse.

1. Innledning

1.1. Mål

Denne overordnede rutinen skal sikre at bestemmelsene i personopplysningsloven, personopplysningsforskriften og andre eksterne bestemmelser overholdes ved utlevering av materiale fra NTNUs datasystemer til politi og påtalemyndighet. Rutinen skal også sikre arkivplikten for slike saker.

1.2. Gyldighetsområde

Denne rutinen gjelder for all henvendelse fra politi og påtalemyndighet om utlevering eller innsyn i data fra NTNUs dataanlegg. Rutinen gjelder både driftsdata og andre data som er lagret på datamaskiner administrert av IT-personale og tilsvarende på andre datasystemer og datamaskiner eid eller disponert av NTNU.

Rutinen dekker ikke forhold der utlevering skjer etter anmeldelse fra NTNU. I disse tilfelle gjelder bestemmelser i NTNUs IT-reglement og i Rutine for innsyn i brukeres e-post og elektronisk lagret materiale.

1.3. Forhold til andre sikkerhetsdokumenter.

I tillegg til denne overordnede rutinen gjelder eventuelle lokale rutiner og bestemmelser som er fastlagt for utlevering av slikt materiale. Lokale rutiner kan ikke spesifisere lavere sikkerhetskrav enn det som er satt opp i de sentrale dokumentene og i dette dokumentet.

Dersom krav med grunnlag i «*Prinsipper for informasjonssikkerhet ved NTNU*», andre sentrale styrende sikkerhetsdokumenter, offentlige lover og forskrifter eller andre relevante rutiner er forskjellig fra kravene i dette dokumentet, gjelder de mest restriktive kravene.

2. Definisjoner

Eid eller disponert av NTNU: (Datamaskiner) innkjøpt og eid av NTNU eller finansiert av andre og stilt til disposisjon for NTNU.

Virksomhetsrelatert materiale: Materiale som er knyttet til gjennomføring av arbeidsoppgaver for NTNU.

Datasystemer og datamaskiner: Både passive systemer som back-up og aktive systemer som filtjenere, arbeidsstasjoner, laboratoriemaskiner og annet utstyr med fillagringsmulighet.

3. Rutiner

3.1. Prinsipper

- Personvernet til brukerne skal sikres.
- For slike saker er det dokumentasjons- og arkivplikt. NTNUs arkivrutiner skal følges. IT-sjefen er formell eier av sakene og har ansvar for at dokumentasjon i saken arkiveres i NTNUs sentrale arkiv. Dersom primærhenvendelsen skjer til enhetsnivået er det meldeplikt til IT-sjefen.
- Alle henvendelser og tilbakemeldinger skal være skriftlig eller loggført. Data kan sikres inntil skriftlig henvendelse foreligger dersom dette er nødvendig.

3.2. Parter

I saker av denne typen skal partene være klart definert.

- Politi eller påtalemyndighet skal være representert av navngitt person.

- NTNU er formelt representert av IT-sjef. Ansvar for det operasjonelle arbeid, skal være delegert til en navngitt person. Dersom henvendelsen skjer til IT-tjenesten eller andre ved enheten skal henvendelsen dirigeres til enhetens ledelse for videre behandling.

3.3. Skriftlig henvendelse

Det skal foreligge skriftlig henvendelse fra politi eller påtalemyndighet ved krav om utlevering av materiale fra driftslogger eller av en brukers elektronisk lagrede materiale. Avsender skal verifiseres. Materiale leveres ikke ut før skriftlig henvendelse foreligger.

3.4. Muntlig henvendelse

Dersom henvendelsen skjer muntlig skal politi/påtalemyndighet gjøres oppmerksom på kravet til skriftlig henvendelse.

Dersom det av bevisårsaker kreves øyeblikkelig aksjon, f.eks. sperring eller sikring av materiale, gjøres dette. Før eventuell sperring eller sikring skal identiteten til den som tar kontakt kontrolleres.

3.5. Rutine for tilbakemelding

All tilbakemelding skal gis skriftlig. Ved muntlig tilbakemelding gis i tillegg en skriftlig tilbakemelding der det framgår at opplysningene også er gitt muntlig. All skriftlig tilbakemelding skal legges i dokumentasjonen av saken. Ved all tilbakemelding skal identiteten til mottaker kontrolleres.

Dersom bruker er identifisert i tilbakemelding skal tilbakemeldingen være unntatt fra offentlighet. I slike tilfeller er det krav om at tilbakemeldinger som e-post blir kryptert.

3.6. Utlevering av driftslogger

3.6.1. Identifisering av bruker fra driftslogger

- Med hjemmel i Ekomloven § 2-9 kan politi eller påtalemyndighet kreve utlevert data fra driftslogg som identifiserer bruker for en gitt «elektronisk kommunikasjonsadresse». Dette forstås som IP-adresse, MAC-adresse eller at oppgitte data fører fram til bruker pålogget tjener eller klientmaskin.
- Tidspunktet kan gis som et vindu. Begrunnelsen for valgt bredde av vinduet skal oppgis i dokumentasjonen av saken.
- Dersom identifiseringen ikke fører fram til bruker men til punktnummer/sted oppgis dette til politi. Det overlates til politi å foreta videre etterforskning ut fra stedsangivelsen.
- Dersom det er usikkerhet når det gjelder identifisering av bruker, skal dette tydelig framgå av svaret til politiet.
- Politi/påtalemyndighet skal kvittere skriftlig for mottatt data fra driftslogg.

3.6.2. Utlevering av andre driftslogger

For utlevering av andre driftslogger kreves hjemmel i lov eller beslutning av politi, påtalemyndighet eller retten.

- Dersom det av tidsmessige årsaker kreves sikring av driftsloggen før en eventuell beslutning av politi, påtalemyndighet eller retten kan foreligge, tas det kopi av de aktuelle driftslogger. Dersom en slik beslutning ikke foreligger innen 14 dager, slettes kopien.
- Driftslogg som skal utleveres brennes på CD/BD-rom eller lignende lagringsmedium i to eksemplarer hvorav den ene oversendes politi/påtalemyndighet. Den andre kopien følger dokumentasjonen i saken.

For driftslogger av mindre omfang kan utlevering skje som vedlegg til e-post eller som utskrift i brev. Politi/påtalemyndighet skal kvittere skriftlig for mottatt driftslogg.

3.7. Utlevering av filer og e-post.

3.7.1. Sikring av materiale etter begjæring fra politi/påtalemyndighet

Politi eller påtalemyndighet kan be om at innholdet på en brukers filområde og e-post sikres på et gitt tidspunkt.

- Dersom politi deltar i arbeidet med sikring skal ikke materialet overleveres til politiet før bestemmelsene for utlevering av materialet gitt i denne rutinen er tilfredsstillt.
- Dersom henvendelsen fra politi eller påtalemyndighet ikke er skriftlig skal den sikrede kopien oppbevares hos den som er bemyndiget i inntil fem virkedager. Dersom ikke skriftlig bekreftelse av anmodningen er mottatt av NTNU innen fem virkedager skal kopien destrueres.
- Når skriftlig henvendelse er mottatt skal kopien oppbevares av IT-sikkerhetsansvarlig ved NTNU eller den han har bemyndiget i inntil 14. kalenderdager. Har ikke politi eller påtalemyndighet i løpet av denne tiden fått samtykke fra brukeren, påvist lovhjemmel, eller framskaffet beslutning fra politi, påtalemyndighet eller retten, skal kopien destrueres.

3.7.2. Utlevering

Utlevering av materiale fra NTNUs dataanlegg krever skriftlig tillatelse fra bruker og eier av materialet, hjemmel i lov eller beslutning av politi, påtalemyndighet eller retten.

- Dersom brukeren har gitt eksplisitt samtykke med angivelse av hvilket materiale eller hvilket filområde som skal utleveres, foretas utlevering av materialet. I de tilfelle materialet eies av andre, kreves også skriftlig tillatelse fra eier. For virksomhetsrelatert materiale kreves skriftlig tillatelse fra leder av brukerens enhet.
- Utlevering skjer ved at det tas to kopier på CD/BD-rom eller annet passende lagringsmedium. Den ene kopien utleveres mens den andre følger dokumentasjonen for saken. Politi/påtalemyndighet skal kvittere skriftlig for mottatt materiale.

3.7.3. Forholdet til brukeren

Så snart saken er avsluttet skal brukeren bli orientert skriftlig om saken med mindre dette ikke er ønskelig ut fra etterforskningsmessige eller andre årsaker, jfr. Personopplysningsloven § 23.

3.8. Dokumentasjon, arkivering

3.8.1. Dokumentasjon av saksgang

Det skal føres logg som dokumenterer saksgangen. Loggen skal ikke inneholde henvisning til brukernavn eller på andre måter kunne brukes for å identifisere brukeren. Loggen skal henvise til sakens arkivreferanse.

Kopi av loggen legges fortløpende i lokalt arkiv ved saksbehandlers enhet. Når saken er avsluttet arkiveres loggen sammen med øvrig dokumentasjon i saken.

3.8.2. Arkivering

Alle dokumenter i saken skal arkiveres i NTNUs sentrale arkiv. NTNUs arkivrutiner følges ved arkiveringen. IT-direktør er eier av saken og ansvarlig for at arkivplikten følges.

3.8.3. *Offentlighet*

Arkivmappen og alle dokumenter med unntak av logg over saksgang skal merkes «Unntatt fra offentlighet».

4. Ansvarlig for dokumentet

Ansvarlig for dokumentet er IT-sjefen.

5. Revisjoner og endringer

Revisjon av dokumentet inngår i den rutinemessige revisjonen av de sentrale rutiner og retningslinjer for Informasjonssikkerhet. Ved behov oppdateres dokumentet fortløpende.