

Forfatter:	RE/PG		
Godkjent av:	odd A. Halseth		
Dokumenttype:	Interne retningslinjer		
Godkjent dato:	22.06.2023	Ikke gyldig etter utskriftsdag	

Lagrings og delingsguide for Nord universitet

Lagringsverktøy	Åpen (grønn)	Beskyttet (gul)	Fortrolig (rød)	Strengt fortrolig (svart)
E-post Office365 (nord.no-konto)	Ja	Ja	Ja (2)	Nei
E-post privat (hotmail, gmail, osv.)	Ja	Nei	Nei	Nei
Lokal harddisk på Nord-administrert PC (jobb-PC)	Ja (4)	Ja (4)	Ja (1,3,4)	Nei
Lokal harddisk på privat PC	Ja	Ja (9)	Nei	Nei
Onedrive for Business	Ja	Ja	Ja (1)	Nei
Prosjektrom (sharepoint)	Ja	Ja	Ja (1)	Nei
Teams (fillagring)	Ja	Ja	Ja (1,6)	Nei
Dropbox (for ekstern-initierte prosjekter)	Ja	Ja	Ja (10)	Nei
Programmer levert via Office365-plattformen (alle, inkl. kommende)	Ja	Ja (7)	Ja (1,7)	Nei
Public360	Ja	Ja	Ja	Ja
FS	Ja	Ja	Ja	Nei
Canvas	Ja	Ja	Nei	Nei
OTRS	Ja	Ja (8)	Nei	Nei
House Of Control	Ja	Ja	Nei	Nei
Basware	Ja	Ja	Nei	Nei
SAP/DFØ/ESS	Ja	Ja	Ja	Nei
Panopto	Ja	Ja	Nei	Nei
Nettskjema	Ja	Ja	Ja (3)	Ja (5)
Nettskjema (diktafon app)	Ja	Ja	Ja (3)	Ja (5)
Nvivo (lokal installasjon)	Ja	Ja	Ja (1,12)	Nei
TSD (Tjeneste for sikker lagring)	Ja	Ja	Ja	Ja

Forfatter:	RE/PG		
Godkjent av:	odd A. Halseth		
Dokumenttype:	Interne retningslinjer		
Godkjent dato:	22.06.2023	Ikke gyldig etter utskriftsdag	

Zoom (undervisning chat)	Ja	Ja	Nei	Nei
Zoom (undervisning video)	Ja	Ja	Nei	Nei
Zoom (Intervju i forskning for ansatte)	Ja (15)	Ja (15)	Ja (15)	Nei
Zoom (opptak forskningsintervjuer)	ja	ja	Ja (16)	Nei
Teams (chat)	Ja	Ja	Nei	Nei
Teams (Video opptak)	Ja	Ja	Nei	Nei
Teams (Live stream)	Ja	Ja	Ja	Nei
Facebook (offisiell konto)	Ja (14)	Nei	Nei	Nei
LinkedIn (offisiell konto)	Ja (14)	Nei	Nei	Nei
"Si fra"-tjenester på Nord.no	Ja	Ja	Nei	Nei
Privat skytjeneste (Dropbox, GoogleDrive, iCloud, osv.)	Ja (14)	Nei	Nei	Nei
Privat pc, mac, nettbrett, telefon	Ja	Nei	Nei	Nei
Private lagringsmedier som harddisker, minnepenner osv.	Ja	Nei (9)	Nei (11,9)	Nei
Filsender Uninett	Ja	Ja	Ja (kryptert)	Nei
Øvring overførig av data (se sikker overføring av data nedefor)				
Transkribering, automatisk transkribering i Microsoft Teams og Word	Ja (14)	Nei	Nei (13)	Nei (13)

1. Røde data trenger ekstra beskyttelse. Det må påseses at krypteringen til enhver tid fyller kravene gitt i informasjonssikkerhetssystemet ved Nord.
2. E-post med røde data skal beskyttes før sending. Vedlegg i beskyttet epost skal ha lik beskyttelse som e-posten.
3. Det skal sikres at røde data ikke lastes ned til eksterne datakilder uten at dataene er beskyttet. Nettskjema diktafonapp kan lastes ned for bruk på privat mobil uten at dette regnes som lagring på privat enhet.
4. Det anbefales generelt ikke å lagre dokumenter på lokal disk på arbeidsstasjonen din. Så lenge du ikke har backup/kopi på nord sine sentrale lagringssystemer.
5. UiO Nettskjema har støtte for å samle inn informasjon og overføre direkte til TSD, som er godkjent for å lagre sorte data. Røde data som samles inn i Nettskjema skal innen rimelig tid slettes, eller flyttes til f.eks. forskningslagring / fellesområde med beskyttelse.

Forfatter:	RE/PG
Godkjent av:	odd A. Halseth
Dokumenttype:	Interne retningslinjer
Godkjent dato:	22.06.2023 Ikke gyldig etter utskriftsdag

6. Gule og røde data kan behandles i Teams dersom Teamet har adgangsbegrensning på dokumentbiblioteket eller informasjonen er beskyttet med annen sikring.
7. Informasjon som skal deles med kolleger, bør legges på et fellesområde, ikke på ditt hjemmeområde.
8. Røde data kan lagres i RT / OTRS etter en egen vurdering. Det skal sikres at røde data ikke ligger i åpne køer. Det skal finnes rutiner for sletting av røde data.
9. Gule data skal som hovedregel ikke behandles på privat maskin. Noe bruk er likevel tillatt gitt at en behandler dataene i web versjon (O365).
10. Må avklares med informasjonseier/behandlingsansvarlig institusjon.
11. Røde data kan lagres på laptop med kryptert disk, kryptert minnepinne eller kryptert ekstern harddisk. Det må påses at krypteringen til enhver tid fyller kravene gitt i informasjonssikkerhetssystemet ved Nord.
12. Ved opprettelse av prosjekt må det velges et lagringsområde og backup som er godkjent for røde data.
13. Transkribering av røde og sorte data skal ikke automatiseres, men gjøres av godkjent leverandør med avtale med Nord universitet.
14. Personopplysninger kan ikke behandles i dette system.
15. Må gjennomføres i henhold til beskrevet rutine i kvalitet i Nord.
16. Kun ansatte ved Nord kan gjøre opptak i Zoom, og opptak må gjøres med Nord-administrert PC. Rutine for bruk av zoom i forskningsintervju skal følges. Filen som lagres ved bruk av Zoom intervju skal lagres på godkjent lagringsområde for røde data.

Forfatter:	RE/PG
Godkjent av:	odd A. Halseth
Dokumenttype:	Interne retningslinjer
Godkjent dato:	22.06.2023 Ikke gyldig etter utskriftsdag

Filesender

- FileSender sørger for enkel overføring av store filer ved bruk av nettleser. Filene kan overføres til én eller flere mottakere. Tjenesten har blitt testet med filer på opptil 1000 GB. FileSender er et sikkert og praktisk alternativ, for eksempel når sending av store filer som e-postvedlegg ikke vil fungere. Tjenesten produseres i sin helhet innenfor norsk UH-sektor, og norsk lovverk ligger til grunn.
- FileSender er et sikkert og praktisk alternativ, for eksempel når sending av store filer som e-postvedlegg ikke vil fungere. Tjenesten produseres i sin helhet innenfor norsk UH-sektor, og norsk lovverk ligger til grunn.
- For mer info: <https://www.unit.no/tjenester/filoverforing-filesender>

Sikker overføring av data

- Sensitive data skal på ingen måte transporteres via fysiske media uten at risikovurdering er foretatt og andre alternative løsninger for overføringen av data er vurdert.
- Gjelder overføringen av data papirdokumenter og disse dokumentene inneholder personsensitive data skal dette vurderes i henhold til risikovurdering og bruk av sikret forsendelse i post eller bud må vurderes.
- Både når det gjelder maskinelt lagret data og papirdata må det tas hensyn og tiltak for at data ikke blir ødelagt pga. ytre påvirkning og klimatiske endringer under overføring.

Datamaskiner

Datamaskiner som inneholder brukerdata skal til enhver tid være sikret mot utilsiktet tilgang.

Kommer datamaskiner på avveie skal det meldes fra til IT avdelingen ved IT-Helpdesk så raskt som mulig for å avgrense eventuelle tap av data.

Mobiltelefoner

Mobiltelefoner skal på lik linje med datamaskiner også holdes under oppsikt til enhver tid.

Hvis IT avdelingen forbeskjedes om at en mobiltelefon er stjålet skal telefonen fjern-slettes for å minimalisere tap og innsyn i data.

Minnepinner, portable harddisker, minnekort og andre portable media

Portable lagringsmedia av denne art skal på ingen måte inneholde personsensitive data uten at dataene er beskyttet. Håndtering og oppbevaring av slike media med brukerdata skal håndteres på lik linje med en bærbar datamaskin eller mobiltelefon.

Forfatter:	RE/PG	
Godkjent av:	odd A. Halseth	
Dokumenttype:	Interne retningslinjer	
Godkjent dato:	22.06.2023	Ikke gyldig etter utskriftsdag