

Rapporttittel: Risiko- og sårbarhetsvurdering av Office 365, Sharepoint, teamsites,  
fillaggring/deling/samarbeid ved NTNU  
Forfatter: Rolf Sture Normann  
Dato: 21.06.2016

Rapporten er unntatt offentlighet i henhold til Offentleglova § 13 og Forvaltningsloven § 13.

# Innhold

Forord	3
Oppsummering	4
Følgende hovedtyper tiltak anbefales iverksatt:	4
Innledning	5
Dato og gjennomføring	5
Systemprofil	6
Resultat fra risiko- og sårbarhetsvurderingen	7
Risikonivå	7
Anbefalte tiltak	8
Vedlegg A Kopi av ROS-regneark	11
Kommentarer fra deltakerne	Feil! Bokmerke er ikke definert.

# Forord

Sekretariat for informasjonssikkerhet i UH sektoren er opprettet av Kunnskapsdepartementet og lagt til UNINETT AS.

Formålet med sekretariatet er å bidra til at UH-sektoren oppnår tilfredsstillende informasjonssikkerhet. Nasjonal strategi for informasjonssikkerhet skal ligge til grunn for sekretariatets arbeid. [https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/nasjonal\\_strategi\\_infosikkerhet.pdf](https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/nasjonal_strategi_infosikkerhet.pdf)

Sekretariatet har utarbeidet en metodikk for gjennomføring av risiko- og sårbarhetsvurderinger, som bygger på den anerkjente standarden ISO/IEC 27005:2005 («Information Security Risk Management»). Denne metodikken er benyttet i risiko- og sårbarhetsvurderingen av LMS.

Mer utfyllende informasjon om risikovurderingsmetodikken som ble anvendt finnes her: <https://www.uninett.no/infosikkerhet/risiko-og-s%C3%A5rbarhetsvurderinger-ros>

# Oppsummering

Risiko- og sårbarhetsvurderingen av Office365 Sharepoint/teamsite/fil/lagring og deling avdekket 29 hendelser som kunne føre til brudd på informasjonssikkerheten.

For 4 av hendelsene ble risikoen vurdert som såpass alvorlig/kritisk (høy risiko) at det er nødvendig med iverksetting av forbedringstiltak. Dette for å unngå at hendelsene påvirker informasjonssikkerheten i systemet på en negativ måte.

For 18 av hendelsene ble risikoen vurdert som middels høy. Dette innebærer at virksomheten også her bør vurdere å iverksette tiltak (Gul).

For 3 av hendelsene ble risikoen vurdert som så liten at tiltak ikke er nødvendig.

For 4 av hendelsene var vi ikke i stand til å vurdere sannsynlighet på grunn av usikkerhet knyttet til den aktuelle hendelsen. Usikkerhetsfaktorene bør sjekkes ut slik at man er oppmerksomme på problemstillingen hendelsen reiser.

## Følgende hovedtyper tiltak anbefales iverksatt:

- Administrativt
  - Tilstrekkelig opplæring av brukere
  - Kultur og holdningsskapende kampanjer, opplysningskampanjer
  - Etablering av rutiner og policy ved bruk
- Teknisk
  - Etablere rollestyrte tilganger
  - Innføre Mobile Device Management (MDM), dette medfører sentral styring av smarttelefoner og nettbrett
  - Benytte ePhorte i større grad for arkivverdig informasjon

Hendelsene og tilhørende tiltak er nærmere beskrevet under punktet «Anbefalte tiltak». Tiltakene er beskrevet på et overordnet nivå. NTNU må selv vurdere og ta nærmere stilling til hvordan de skal utformes og iverksettes slik at man oppnår tilfredsstillende informasjonssikkerhet.

# Innledning

## Dato og gjennomføring

ROS-workshopen ble holdt 24. mai 2016 på NTNU, Gløshaugen. Deltakerne var fra NTNU med observatører fra UNINETT UH\_Sky programmet. ROSen ble fasilitert av UH-sektorens sekretariat for informasjonssikkerhet hos UNINETT.

På grunn av at man i ROS-rapporten beskriver sensitive forhold vedrørende bruken av Office365, kan deler av rapporten unntas offentlighet i henhold til Offentleglova § 13 og Forvaltningsloven § 13. Det anbefales at man vurderer om det er forhold i rapporten som omtaler enheter/avdelinger på en slik måte at det kan skade informasjonssikkerheten om den skulle komme på avveie.

Rapporten er utarbeidet av Rolf Sture Normann og Tommy Tranvik ved UH-sektorens sekretariat for informasjonssikkerhet med innspill fra deltakerne.

## Deltakere

Navn	Rolle	Institusjon
Ole Langfeldt		NTNU
Snorre Jenssen		NTNU
Rolf Sture Normann	Sekretariat for informasjonssikkerhet i UH sektoren	UNINETT
Tommy Tranvik	Sekretariat for informasjonssikkerhet i UH sektoren	UNINETT

## Systemprofil

Tjeneste/System	LMS
Risikoeier	
Virksomhetsområde	
Utbredelse	
Beskrivelse	Office365 Sharepoint/Teamsite lagring og deling av dokumenter
Leverandør	Microsoft
Driftes av	Microsoft

# Resultat fra risiko- og sårbarhetsvurderingen

## Risikonivå

Det ble i ROSen identifisert 29 risikoelementer (uønskede hendelser). Fordelingen mellom risikonivåene er vist i tabellen under.

Risikonivå	Høy	Medium	Lav	Udefinert
Antall	4	18	3	4

Risikoelementet med lav risiko (grønn) vil ikke vurderes spesielt i denne rapporten men tas med slik at de evt. kan vurderes på nytt ved senere risiko- og sårbarhetsvurderinger.

Risikoelementene er for oversiktens skyld markert i matrisen under.

Konsekvens	4 Svært høy	8, 17			
	3 Høy	3, 10, 24	7	9,14,26	16
	2 Moderat	18, 22, 23	2, 11, 12, 20, 25, 29	5, 15	
	1 Liten			4, 5, 6, 19	
		1 Lav	2 Moderat	3 Høy	4 Svært høy
Sannsynlighet					

### Anbefalte tiltak

Tiltakene som er presentert i tabellene ble identifisert under workshopen. Det er risikoeiernes ansvar å eventuelt komme med ytterligere tiltak eller endre de foreslåtte tiltakene.

Tiltakskortene baserer seg på uønskede hendelser som ble vurdert med risikofaktor 5 eller høyere. Dette medfører alle høyere middels, (Gul) og alle med høy risikoverdi (rød).

Tiltakskort nr. 1			
Organisasjon:	NTNU	Risiko	Tiltak
Tiltakstype:	Administrativt	Uvedkommende får tilgang til sensitive data	Gjentagende påminnelser til brukere.
Risikoelement:	16	Deling av brukernavn/passord på grunn av holdninger eller mangelfull kompetanse/bevissthet	
Risikonivå:	Høy		
Anm: Det er laget passordpolicy ved NTNU			

Tiltakskort nr. 2			
Organisasjon:	NTNU	Risiko	Tiltak
Tiltakstype:	Administrativt	Mangelfull sikring av forskningsdata, konfidensialitet	IRM, policy for behandling av forskningsdata, info til forskere
Risikoelement:	9		
Risikonivå:	Høy		
Anm: Informasjon via banner på O365 åpningsside og informasjon om sikkerhet nederst på denne siden.		Sensitive forskningsdata lagres i O365 pga manglende informasjon til brukermiljøet om retningslinjer for hvor ulike type data skal eller kan lagres.	

Tiltakskort nr. 3			
Organisasjon:	NTNU	Risiko	Tiltak
Tiltakstype:	Teknisk	Sensitive data på avveie  Mangelfull sikkerhet på håndholdt/bærbart IT-utstyr pga. lagring av passord på enheten. Dermed er det bare eventuell skjermlås som hindrer uvedkommende å få tilgang til data som ellers er underlagt passordpolicy. Smarttelefoner/nettbrett kan lett mistes eller bli stjålet.	Innføre MDM, Mobile Device Management. Sentral styring av smarttelefoner/nettbrett.
Risikoelement:	14		
Risikonivå:	Høy		
Anm: Det er laget passordpolicy ved NTNU			



Tiltakskort nr. 4			
Organisasjon:	NTNU	Risiko	Tiltak
Tiltakstype:	Administrativt	Data er utilgjengelig	Data av juridisk eller forvaltningsmessig verdi må over i ePhorte (jf NTNUs arkivplan og regler for bevaring/kassasjon).
Risikoelement:	26	Manglende historiske back-up, data slettes etter 90 dager	
Risikonivå:	Høy		
Anm:			

Tiltakskort nr. 5			
Organisasjon:	NTNU	Risiko	Tiltak
Tiltakstype:	Administrativt	Sensitive dokumenter eller opplysninger deles med feil person eller feil gruppe. Kan også føre til uautorisert endring/sletting.	Brukeropplæring og informasjon
Risikoelement:	1		
Risikonivå:	Middels		
Anm:		Brukerfeil - Uriktig bruk av "share with everyone"-mappen på grunn av manglende kompetanse om hvordan denne delingsmuligheten fungerer.	

Tiltakskort nr. 6			
Organisasjon:	NTNU	Risiko	Tiltak
Tiltakstype:	Administrativt	Uautorisert tilgang til sensitive data etter at tilgangen skulle vært avsluttet, kan misbrukes	Innføre rollestyrt tilgang
Risikoelement:	7		
Risikonivå:	Middels		
Anm: Satt i gang tiltak for automatisk sletting av brukere		Brukertilganger til dokumenter eller data endres ikke når personer endrer rolle/stilling internt eller slutter. Dermed blir tilganger til data man ikke skal ha tilgang til liggende igjen.	

Tiltakskort nr. 7			
Organisasjon:	NTNU	Risiko	Tiltak
Tiltakstype:	Administrativt/teknisk	Uautorisert tilgang til systemet.  Administrator-tilganger slettes ikke når administrator slutter i stillingen. Ref. punkt 7 over h(tiltakskort nr. 6).	Rollestyrt tilgang, begrense administrator rettigheter.
Risikoelement:	8		
Risikonivå:	Middels		
Anm:			

Tiltakskort nr. 8			
Organisasjon:	NTNU	Risiko	Tiltak
Tiltakstype:	Administrativt/teknisk	Uvedkommende får tilgang til sensitive data  Brukernavn og passord på avveie, fanges opp pga. at O365 er tilgjengelig fra internett. For eksempel dersom man sitter på en internettcafe, kan det være skadevare på denne maskinen som brukeren ikke har kontroll over. (key-logger)	Policy-basert lagring, informasjon og brukeropplæring
Risikoelement:	15		
Risikonivå:	Middels		
Anm: Etablert løsning for varsling av slike hendelser i O365			

Tiltakskort nr. 9			
Organisasjon:	NTNU	Risiko	Tiltak
Tiltakstype:	Administrativt	Uvedkommende får tilgang til sensitive identitetsdata  Data om personer med skjult identitet kan bli tilgjengeligjort gjennom Office365	Bevisstgjøring av brukere
Risikoelement:	17		
Risikonivå:	Middels		
Anm:			

# Vedlegg A Kopi av ROS-regneark

Risiko- og sårbarhetsvurdering (ROS)							
Tjeneste/System		Office 365, NTNU					
Nr.	Risikoelement	Sårbarheter/ svakheter	Eksisterende beskyttelsestiltak	Eksisterende kontrolltiltak	Vurdering		
					S	K	Risiko
16	Uvedkommende får tilgang til sensitive data	Deling av brukernavn/passord på grunn av holdninger eller mangelfull kompetanse/bevissthet	Det er laget passordpolicy ved NTNU		4	3	7
9	Mangelfull sikring av forskningsdata, konfidensialitet	Sensitive forskningsdata lagres i O365 pga manglende informasjon til brukermiljøet om retningslinjer for hvor ulike type data skal eller kan lagres	Generell informasjon via banner på O365 loginnside og info om sikkerhet nederst på siden		3	3	6
14	Sensitive data på avveie	Mangelfullt sikkerhetsnett på NTNU, utstyr pga. lagring av passord på enheten. Dermed er det bare eventuell skjerm-lås som hindrer uvedkommende å få tilgang til data som	Det er laget passordpolicy ved NTNU		3	3	6
26	Data er utliggjengelig	Manglende historiske back-up, data slettes etter 90 dager			3	3	6
1	Sensitive dokumenter eller opplysninger deles med feil person eller feil gruppe. Kan også føre til uautorisert endring/sletting.	Brukerfeil - Urliglig bruk av "share with everyone"-appen på grunn av manglende kompetanse om hvordan denne delingsmuligheten fungerer.			3	2	5
7	Uautorisert tilgang til sensitive data etter at tilgangen skulle vært avsluttet, kan misbrukes	Brukerfeil - Uautorisert bruk av data endres ikke når personer endrer rolle/stilling internt eller slutter. Dermed blir tilgang til data man ikke skal ha tilgang til liggende igjen.	Satt i gang tiltak for automatisk sletting av brukere		2	3	5
8	Uautorisert tilgang til systemet.	Admin-tilganger slettes ikke når admin slutter i stillingen. Ref. punkt 7, over.			1	4	5
15	Uvedkommende får tilgang til sensitive data	Brukerfeil - Uautorisert bruk av data endres ikke når personer endrer rolle/stilling internt eller slutter. Dermed blir tilgang til data man ikke skal ha tilgang til liggende igjen.	Etablert løsning for varsling av slike hendelser i O365		3	2	5
17	Uvedkommende får tilgang til sensitive identitetsdata	Data om personer med skjult identitet kan bli tilgjengelig gjort gjennom Office365			1	4	5
2	Sensitive dokumenter eller opplysninger deles med feil person eller feil gruppe. Kan også føre til uautorisert endring/sletting.	Sikkerhetsnett i Office 365 gjør at data i "share with everyone"-appen kan bli tilgjengelig gjort for uvedkommende. Brukerne er ikke oppmerksom på dette på grunn av manglende kompetanse.			2	2	4
3	Uvedkommende får tilgang til og kan endre/slette viktige dokumenter/ opplysninger	Brukerfeil - Feil tildeling av lese- og redigeringsrettigheter på grunn av manglende kompetanse kompetanse/opplæring.			1	3	4
4	Mangelfull tilgjengelighet til data	Brukerfeil - Feil tildeling av lese- og redigeringsrettigheter på grunn av manglende kompetanse kompetanse/opplæring.			3	1	4
5	Integritets- eller tilgjengelighetsbrudd	Ulike rutiner for bruk avhengig av hvilket klient utstyr som benyttes - mobil, windows-pc, mac-pc osv. Kan føre til brukerfeil, for eksempel usikkerhet omkring hvor dokumenter lagres.			3	1	4
6	Mangelfull tilgjengelighet	Ved sletting av brukere i AAD, vil informasjonen vedkommende bruker har i OneDrive slettes. Dette kan for eksempel gjelde studenter i permisjon og som ikke betaler semesteravgift, eller ikke er klar over at manglende semesteravgift medfører sletting av bruker.			3	1	4
10	Sensitive data på avveie	Romeler kan gi sin private konto fulle rettigheter til dette rommet, vil dermed kunne ha full tilgang til et rom/site selv om vedkommende ikke har bruker i NTNU lenger.	Dette vil være synlig for andre deltakere i rommet		1	3	4
11	Uvedkommende får tilgang til sensitive data	Inviterer til ekstern bruker inn i prosjektmiljø. Kan skje på to måter, anvende delingsfunksjonen inne i Office365, eller kolierer og distribuerer URL til rommet via			2	2	4
12	Uvedkommende får tilgang til sensitive data	Feil dokument kopieres fra OneDrive til pc til prosjektmiljø på OneDrive. Utsiktstet			2	2	4
19	Viktige data er utliggjengelig	Hedetid, blant annet pga at oppgradering eller endring i tjenesten ikke varsles. Kan gjelde nedetid hos Microsoft, forskningsnettverk eller NTNUs eget nettverk.			3	1	4
20	Viktige data er utliggjengelig	Kunde eller leverandør utsettes for DDoS-angrep, påloggingstjenesten er nede, Feide er nede osv.			2	2	4
24	Uvedkommende får tilgang til sensitive data	Felikonfigurasjon hos Microsoft fører til flyt av data mellom tenants/ulike kunder			1	3	4
25	Integritets- eller tilgjengelighetsbrudd	Infiserte klienter kan spre ødeleggende programvare til OneDrive via sync (eller infiserte dokumenter)	Mindre syncing av online-dokumenter ved NTNU		2	2	4
29	Manglende sporbarhet på brukeraktiviteter	Mangelfull aktivitetsslogging i Office365			2	2	4
18	Uvedkommende får tilgang til sensitive data, uautorisert endring/sletting	Nettleser lagrer passord (lagrer sesjonen) slik at uvedkommende kan logge seg inn på OneDrive-kontoen til tidligere bruker, spesielt pc som er plassert i auditorium eller bibliotek			1	2	3
22	Manglende kontroll med data, mulighet for brudd på konfidensialitet, integritet eller tilgjengelighet (NTT). Brudd på regulatoriske krav til bruk av databehandling	Lokal administrator kobler sammen tjenester med Office365 uten at dette er kvalitetssikret eller vurdert. (Big Data)	Gjelder bare for globale administratorer		1	2	3
23	Data er utliggjengelig (datatapi)	Ikke lokal back-up hos NTNU og back-up hos Microsoft forsvinner. Det er ingen sikkerhetskopiering ut over det som Microsoft	Microsoft kan restore data to uker tilbake i tid		1	2	3
13	Sensitive data på avveie	Data synkroniseres mellom OneDrive og lokalPC kan endres. Oppsettet kan endres til å synkronisere data som kan bli tilgjengelig for annen bruker, så som eksempelvis data			0		
21	Usikkerhet om sletting av data ved avslutning av tjenesten	Usikkerhet om hva som er avtalt med Microsoft mht. dette			0		
27	Data på avveie	Microsoft/O365 mer utsatt for fishing-angrep pga kjent merkevare			0		
28	Mangelfull kontroll med datakaskasjon	Muligheter til Innsyn i datakaskasjon, usikkerhet om hvor data befinner seg og hvem som har eller kan ha tilgang til data. "Where is my data" kan være mangelfull.			0		

37	Konfidensialitetsbrudd (tilgang på tvers av tenants)	Mangelfull datasegmentering hos leverandør. Data kan flyte mellom organisasjoner ved for eksempel en feilkonfigurasjon.			2	3	5	
38	Mangelfull tilgjengelighet.	Manglende båndbredde i perioder med stor trafikk, for eksempel ved eksamen.			3	2	5	
7	Manglende muligheter for dataportabilitet. Informasjon kan gå tapt eller lagres for lenge.	Mangelfull sletting av data i systemet eller langtidslagring av data i system som burde vært slettet eller flyttet.			2	2	4	
9	Manglende systemtilgang i kritiske perioder (bl.a. eksamen, oppgaveinnlevering).	Kan ha ulike årsaker, for eksempel hacking, DDOS, Manglende nettilgang, Systemkrasj hos leverandør etc.			2	2	4	
10	Ikke tilgjengelige data.	Hacking, DDOS. Se punkt 9.			2	2	4	Redundans via Uninett.
20	Mangelfull datakontroll.	Manglende muligheter til styring av databehandling hos leverandør, for eksempel revisjon og sletting av data ved avslutning av tjenesten.			1	3	4	
22	Data på avveie.	Kompleks dataflyt ved bruk av tredjepartsapplikasjoner (bl.a. plagiatkontroll), vanskelig å kontrollere hvor data behandles, for eksempel eksport/lagring.			2	2	4	Demonstrere hvordan integrasjoner fungerer.
23	Mangelfull datakvalitet eller tilgjengelighet.	Autoriserte integrasjoner mellom systemer fungerer ikke som forutsatt.			3	1	4	
26	Manglende tilgjengelighet.	Problemer med tilgang til data i systemet fordi det ikke fungerer mot visse typer nettlesere eller versjoner.			3	1	4	Krav til hvilke nettlesere systemet må støtte (inn i SLA). Aktiv forvaltning av systemet.
42	Manglende tilgjengelighet.	Manglende supportkapasitet hos leverandør, ikke tilgjengelig personell ved alvorlige hendelser.			2	2	4	
32	Brudd på KIT	Begrensede muligheter til å gjennomføre sårbarhetstesting (ex. Penetrasjonstest) hos leverandør.			1	3	4	
33	Brudd på KIT	Mangelfull kvalitetsikring av grunndata hos institusjonen eller hos leverandør, for eksempel som følge av oppdatering av data i kilde systemet.			1	3	4	Beskrive hvordan grunndata synkes, roll-back.
11	ID-tyveri.	Brukernavn/passord på avveie og utnyttes til uautorisert tilgang. Uautoriserte har skaffet seg tilgang til en som er slettet av annen bruker.			1	2	3	Tofaktorausentisering
18	Uautorisert datatilgang.	Eksemplet er hentet fra bytte av underviser hvor data tidligere underviser hadde slettet, men som i realiteten lå i papirkurven.			2	1	3	
19	Manglende datakontroll/konfigurasjonskontroll.	Leverandør integrerer systemet mot tredjepartsapplikasjoner uten at dette er godkjent av institusjonen.			1	2	3	Klare ansvars- og myndighetsforhold, avtaleregulering (varslingsrutiner).
34	Brudd på regulatoriske krav.	Leverandør blir kjøpt av ett selskap utenfor EU/EØS.			1	2	3	
35	Manglende tilgjengelighet.	Må skifte system på kort frist, for eksempel pga. konkurs, endrede rammevilkår eller strukturendringer i sektoren.			1	2	3	
36	Brudd på regulatoriske krav.	Manglende eller mangelfull databehandleravtale, eller manglende hjemmel til overføring av data til tredjeland.			1	2	3	
39	Myndighetstilgang til data.	Utenlandske myndigheter krever tilgang til data lagret utenfor kongerikets grenser.			1	2	3	
44	Brudd på KIT	Mangelfull tiltak hos leverandør mot spredning av adeleggende programvare.			1	2	3	
31	Mangelfull tilgjengelighet og brudd på regulatoriske krav.	Systemet blir så omfattende/komplisert at institusjonen mister oversikt over data og hvor data flyter til/fra.			1	2	3	Problemstilling man bør være oppmerksom på, vurderes ikke.
16	Uautorisert datatilgang.	Manglende muligheter for tilstrekkelig tilgangsstyring til data med ulike konfidensialitetsbehov.					0	Sett gjerne verdi for konsekvens!
21	Lock-in (låsing til leverandør).	Manglende dataportabilitet.					0	Problemstilling man bør være oppmerksom på, vurderes ikke.
24	Brudd på regulatoriske krav.	Ulike sikkerhetskrav hos forskjellige institusjoner/lokale enheter. Oppstår ved at alle håndteres likt når behovet for sikkerhet er forskjellig hos ulike institusjoner eller lokale enheter. (medisinstudier etc.)					0	Problemstilling man bør være oppmerksom på, vurderes ikke.
41	Uautorisert datatilgang.	Feil tilgangsstyring pga. komplisert rettighetsstyring i systemet.					0	Jf pkt 1.