NTNU

ROS – Office 365 Oppsummering

NTNU

1 BAKGRUNN

NTNU har som svært mange andre organisasjoner tatt et steg ut i skyen med Office 365. Og det er etter hvert bygget mange viktige tjenester for NTNU på denne skyplattformen.

Dersom man ser på trendene innen IT globalt så er NTNU på den samme veien som majoriteten av virksomhetene er styrt av de største skyleverandørene som Amazon, Microsoft, IBM etc.

I den videre prosessen med å adoptere skytjenester så vil nok GÉANT avtalen og Uninett sin avtale bli relevant også for NTNU.

Sett i lys av IT trendene og hvilken rolle NTNU har i samfunnet som en viktig aktør innen bruk og opplæring i teknolog, så er det viktig at NTNU tar i bruk skytjenester på en sikkerhetsmessig gjennomtenkt måte.

Som en del av arbeidet med å ta i bruk Office 365 tjenestene ved NTNU så har det blitt gjennomført forskjellige ROS analyser for de enkelte tjenestene. NTNU IT v/Strategi og styring har vært bestillere av disse analysene.

Uninett har bistått i deler av dette arbeidet og denne oppsummeringen som er utarbeidet av en arbeidsgruppe ved NTNU (Se 1.2) har som formål å trekke frem anbefalte tiltak som NTNU bør gjennomføre for å håndtere risikoene på en akseptabel måte.

1.1 OM ARBEIDET SOM ER UTFØRT

Uninett har fasilitert og gjennomført 2 adskilte ROS analyser i tett samarbeid med NTNU. Resultatene fra disse to samlingene er dokumentert i en samlerapport som dere finner under dokumentreferansene. Dokumentet tar utgangspunkt i samlerapporten fra Uninett og det er derfor en forutsetning at denne er lest og forstått. – Se punkt 1 i 0 Dokumentreferanser.

Den første ROS analysen som Uninett gjennomførte i samarbeid med NTNU var knyttet til innføringen av SharePoint med TeamSites og OneDrive som arenaer for samhandling.

Den andre ROS analysen var knyttet til Exchange online for ansatte ved NTNU.

I forbindelse med denne prosessen ble det satt ned en arbeidsgruppe som har i mandat å se på Uninetts forslag til tiltak for å redusere risikoer samt komme med innstillinger til praktisk implementering av anbefalte tiltak ved NTNU.

1.2 RÅDGIVENDE ARBEIDSGRUPPE

Uninett ved Rolf Sture Normann som leder, har gjennomført og utarbeidet rapportene fra de aktuelle samlingene.

Følgende personer ble i fellesskap valgt til å delta i det videre arbeidet for å oppsummere ROS analysene og foreslå konkrete tiltak ved NTNU for å håndtere de viktigste risikoene.

Det ligger også i mandatet til arbeidsgruppen å gi råd til ledelsen i forhold til videre utnyttelse av

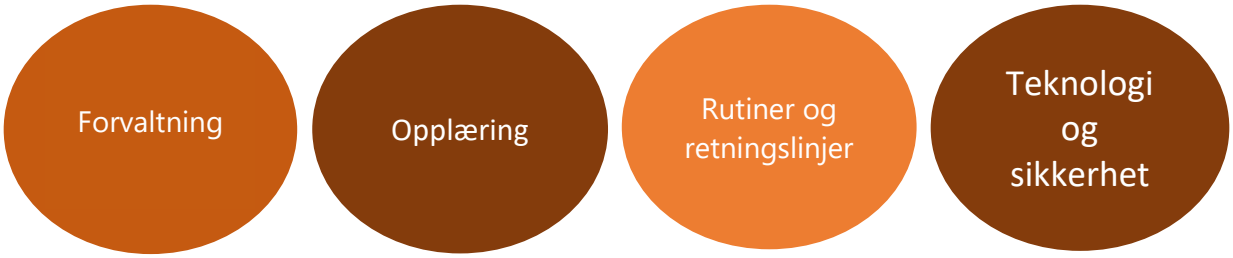
Office 365 plattformen for NTNU knyttet til epost i sky for ansatte, samt det å utnytte plattformen til håndtering av konfidensielt innhold i henhold til policy for informasjonssikkerhet.

Navn	Rolle
Vebjørn Slyngstadli	Sikkerhet
Per Atle Eliassen	Arkitekt – Strategi og styring
Ole I. Langfeldt	Arkitekt – Strategi og styring
Ragnhild Syrstad Wold	Forvaltning
Snorre Jensen	Prosjektleder/koordinator

1.3 OPPSUMMERING OG ANBEFALINGER

Denne rapporten er et forsøk på å foreslå tiltak for å redusere risiko ved å flytte e-post til Office 365. Tiltakene som foreslås er ment som minimumstiltak for å kunne ivareta informasjonssikkerheten.

Tiltak er knyttet til disse områdene



Gruppa ikke har foretatt en kost/nytte vurdering. Det anbefales på det sterkeste at dette gjøres da Microsoft har varslet endringer i lisensmodellen. Det er også et viktig moment at ved å legge flere tjenester i Office365, så knytter man et enda sterkere bånd til leverandør. Dette vil på sikt gjøre det enda vanskeligere å bytte leverandør. Dette er tatt hensyn til ved at vi anbefaler beskrivelse av en «exitstrategi».

Andre organisasjoner i sektoren som har migrert e-post til Office365 er bla. Nord, UiA, HiOA og UiT. I ROS rapport fra Nord så er det så vidt vi kan se ikke vurdert risikoen i forhold til e-post og klassifisering av informasjon. Men de har vurdert risikoen for at sensitive data kan komme på avveie som høy.

Et av de viktigste tiltakene som foreslås er å utvide plattformen til å kunne håndtere fortrolig informasjon. Dette vil også gjøre det mulig å ta i bruk SharePoint, Teams og andre tjenester innen flere områder.

Anbefaling

På grunnlag av ROS analysen som er foretatt kan vi anbefale en migrering av e-post for ansatte til Office 365 for NTNU, forutsatt at man gjennomfører anbefalte tiltak i denne rapporten. Gruppa anbefaler ikke en migrering til Office365 dersom man velger å se bort fra tiltakene som gjør at NTNU også kan lagre fortrolig informasjon. Bakgrunnen for dette er at det i dag ligger mye informasjon i e-post som vil havne inn under kategorien fortrolig.

NTNU

1.4 DOKUMENTREFERANSER

Dette dokumentet referer til andre kilder i flere sammenhenger. Referansene til kildene finner dere i tabellen under her.

Rapporten refererer også til NTNU sin policy for informasjonssikkerhet. Se innsida lenke: https://innsida.ntnu.no/wiki/-/wiki/Norsk/Informasjonssikkerhet

Dokument	Forklaring	Peker
1. Uninett samlerapport (Inkludert Exchange online)	Samlerapporten fra Uninett på gjennomførte ROS analyser ved NTNU	Lenke til Uninett Rapport her
2. Forvaltningsdokument/Styrende dokument	Styrende dokument for Office 365. UH-Sky versjonen.	Lenke
3. Regnearkene med vurderinger.	De forskjellige regnearkene fra samlingene ligger på TeamSite for ROS analysen. - *Unntatt offentlighet*	NA
4. Delrapport 1. Uninett	ROS gjennomgang med fokus på SharePoint og OneDrive - *Unntatt offentlighet*	NA
5. Handlingsplan Office 365	Office 365 Handlingsplan 2017 – 2018. - *Unntatt offentlighet*	NA
6. God praksis for lagring	Det jobbes med forankring av «God praksis» for lagring og informasjonsflyt ved NTNU. - *Unntatt offentlighet*	NA

2 OFFICE 365 VED NTNU

Office 365 ved NTNU er implementert i form av en enkeltstående Office 365 Tenant som er koblet sammen med NTNU sin Active Directory katalogtjeneste. Dette betyr at brukerkontoer og grupper i Active Directory synkroniseres ut til Azure Active Directory som er tilknyttet NTNU sin Office 365 Tenant.

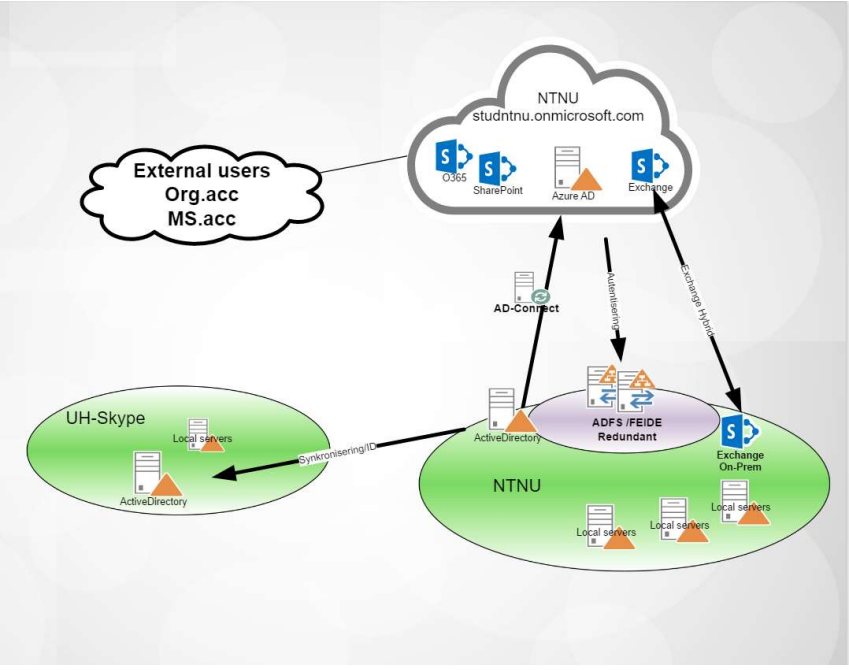
NTNU sin Office 365 Tenant er lokalisert i Microsoft sine datasentre i EU.

Foreløpige føringer/policyer som gjelder for bruken av Office 365 tjenestene ved NTNU er blant annet:

Tjeneste	Studenter	Ansatte
Exchange Hybrid	Exchange Online (365)	Exchange On-premise (Lokalt)
Skype for Business	Skype Online	UH-Skype
SharePoint	SharePoint Online	SharePoint online og On-premis
OneDrive for business	Office 365	Office 365
Øvrige Office 365 tjenester	Office 365	Office 365

2.1 TEKNISK SKISSE

Skisse over infrastruktur knyttet til Office 365 v/NTNU. Dette viser at Skype for Business ligger i Uninett sin skyløsning.



NTNU

2.2 UTNYTTELSE AV PLATTFORMEN OFFICE 365

Office 365 som en plattform for samhandling og digitalisering benyttes i dag aktivt ved NTNU.

Kort tabell med oversikt over de viktigste tjenestene og løsningene som benyttes aktivt i dag.

Tjeneste	**Antall brukere /Brukergrupper**	**Volum**
OneDrive for Business	Alle brukere. Studenter og ansatte v/NTNU	➢ 60 Terrabyte lagring Mye brukt.
TeamSites – Samhandlingsrom på SharePoint	I overkant av 2000 samhandlingsrom for ansatte og studenter	I overkant av 2000 TeamSites. Microsoft Groups og Teams er også sterkt økende.
Exchange Online for studenter	Epost for samtlige studenter	E-post studenter mye brukt, men mange videresender til gmail etc
Læringsportalen – e-læring og kursadministrasjon	Ansatte og studenter. - Primært ansatte	Brukes aktivt. Statistikker ikke tatt ut
OrgSite – avdelingsrom for organisasjonen	Begrenset til gjennomført pilot	Variabel bruk
Kvalitetssystem for Eiendom	Begrenset til Eiendom	Brukes aktivt.
Campus Prosjektet – prosjektportefølge	Ca 35 brukere	25 Aktive prosjekter.
Teams og Groups	Relativt mye brukt.	Statistikk ikke hentet ut.

3 UNINETT SAMLERAPPORT HOVEDPUNKTER

Det ble i de to ROS analysene avdekket til sammen 15 risikoer med verdien 6 eller høyere. Dette er å betrakte som høy risiko og tiltak bør adresseres.

Uninett har kategorisert elementene i følgende hovedkategorier.

Her finner dere de viktigste utdragene fra samlerapporten: - Fullstendig rapport finner dere her:

3.1 MANGLENDE FORVALTNINGSREGIME

NTNU bør etablere et godt forankret forvaltningsregime for løsningen. Mange av hendelsene peker på svakheter knyttet til ansvar og myndighetsforhold. Dette gjelder både internt på NTNU men også mellom NTNU og Microsoft som databehandler. Det er også viktig at NTNU gjør seg i stand til å forvalte sitt ansvar som behandlingsansvarlig overfor Microsoft som databehandler i henhold til gjeldende regelverk. Hendelser knyttet til manglende oppfølging av løsningen inklusive leverandør (Microsoft), ble ved flere anledninger nevnt under arbeidsmøtene.

Endringer i rammebetingelser hos Microsoft, for eksempel ved omorganiseringer/oppkjøp, økonomiske nedgangstider eller lignende må kunne håndteres av NTNU. Dette medfører at NTNU etablerer en klar exitstrategi som gjør NTNU i stand til å gjøre endringer av leverandør uten at dette skaper kritiske situasjoner.

3.2 MENNESKELIG FEIL AV BRUKER

Løsningen vil medføre at brukerne kan dele informasjon med andre. Enten dette er eksterne brukere eller interne brukere. Flere av hendelsene går ut på at brukeren gjør feil ved deling av dokumenter, eller feil ved deling av tilganger. Man kan også glemme å ta bort tilganger som tidligere er gitt. Ved en skyløsning som Office365 kan brukerne selv sette opp tilganger til dokumenter eller mapper. Dette innebærer at brukerne må være årvåkne både ved tildeling av rettigheter og å sjekke hvem som har tilgang til dokumentene.

Brukere kan også feilaktig laste opp dokumenter i skyen som ikke egner seg til å legge ut i skyen. Det kan også være brudd på regulatoriske eller avtalemessige forhold. Oppdragsforskning med spesielle

krav til beskyttelse kan være eksempel på slik informasjon. Mange av hendelsene som kom frem handlet om disse forhold.

Brukernavn og passord på avveier er en hendelse som kan få store konsekvenser i en slik løsning. Dersom man har en konto som er på avveier vil man kunne oppleve at en ondsinnet aktør kan ha lagt inn egne tilganger eller delt områder som senere kan utnyttes selv om eieren av brukerkontoen skifter passord.

3.3 BÆRBARE ELLER HÅNDHOLDTE ENHETER

Det benyttes stadig mer bærbare eller håndholdte enheter til behandling av informasjon. Smart-telefoner eller nettbrett med internettilgang er typiske eksempler som de fleste har tilgang på. NTNU har ingen styring av håndholdte enheter og hvorvidt de er sikret med pinkode eller passord med tilsvarende styrke som man krever i systemløsningene som er tilgjengelig via denne. Det er ofte slik at dersom man først får åpnet en håndholdt enhet, har man direkte tilgang til de applikasjoner som ligger i denne, ofte uten å måtte skrive passord pånytt. Dersom en håndholdt enhet blir mistet eller stjålet, er det derfor stor sannsynlighet for og konsekvens ved at denne blir utnyttet.

3.4 SIKKERHETSKOPIERING

Løsningen til Microsoft inneholder ikke en reell sikkerhetskopiering. Men på grunn av redundans og robusthet innebygget i løsningen, har man mulighet til å få tilbake data som er opptil 90 dager gamle. NTNU vurderte dette som en stor risiko, og her må man også vurdere muligheten for evig tap av data.

3.5 AVHENGIGHET TIL MICROSOFT

NTNU har allerede med dagens løsning erfart at det tar mye lengre tid å rette opp kritiske feil i systemet. For eksempel dersom man oppdager en «phising» angrep som kan skade NTNU, vil dette kunne ta uakseptabel lang tid å få rettet på via Microsoft. Her er det stor forskjell på lokal løsning og sky-løsning. Dette å ikke kunne respondere raskt nok på hendelser fordi man er avhengig av kapasiteten til en ekstern aktør er vurdert til å ha en høy risiko.

Et annet forhold som ble diskutert er at man er avhengige av å kjøre løsningen slik Microsoft har bestemt. Dette medfører at det kan være vanskelig å etablere egne nødvendige sikkerhetstiltak, fordi dette ikke er en del av Microsoft sitt tilbud.

3.6 MANGLENDE BRUKEROPPLÆRING

Mange av hendelsene som ble diskutert på arbeidsmøtene skyldtes at brukerne mangler kompetanse eller informasjon om løsningen. Hvor lagres dataene?, hvordan sikrer jeg at jeg deler de riktige dokumentene/mappene med riktige brukere?, og hva kan man faktisk bruke Office365 løsningen til?

Det kom også frem uønskede hendelser som skyldes manglende kompetanse fra de som jobber på IT-drift.

3.7 KATEGORISERING AV TILTAK

Det foreslås at det iverksettes forbedringstiltak innenfor følgende tiltakskategorier:

1. ***Forvaltning og overvåking: God forvaltning av tjenesten***
2. ***Opplæring: Opplæring til brukere, inkludert driftspersonell***
3. ***Rutiner og Retningslinjer: Etablering av rutiner og retningslinjer.***
4. ***Tekniske forbedringstiltak.***

3.8 UNINETT – KONKRETE TILTAKSFORSLAG

Forslagene fra Uninett til hvilke tiltak NTNU bør iverksette for å håndtere risikoene.

1) NTNU bør etablere et forvaltningsregime som er forankret i toppledelsen for Office365 løsningen. Mange av hendelsene peker på svakheter knyttet til ansvar og myndighetsforhold og etablering av rutiner og retningslinjer.
2) Skaffe seg oversikt over informasjonsverdier og innføre en klassifisering av informasjon.
3) Etablere rutiner for sikkerhetsopplæring, holdningskampanjer for å skape en god sikkerhetskultur.
4) Etablere et regime for å styre bærbare eller håndholdte enheter, eller sørge for at slike ikke reduserer den sikkerheten som vanlige klienter er underlagt.
5) Vurdere behov for backup av data i løsningen gjennom 3. partsverktøy

NTNU

6) Redusere avhengigheten til en leverandør, i dette tilfellet Microsoft ved å lage en strategi for hvordan man går ut av, eller endrer leverandør. Her vil også kontinuitetsplaner være viktige.
7) NTNU bør sørge for å gi brukerne tilstrekkelig opplæring for å minimalisere sannsynligheten for at de vil gjøre feil.
8) Etablere tekniske løsninger som tilbys for å kryptere informasjon og hindre utilsiktede feil.

Generelt sett bør NTNU som minimum vurdere å etablere tiltak for alle hendelser med risikoverdi 6 eller høyere. Det er også viktig at hendelser med lavere risikoverdi enn 6 blir vurdert, enten med å etablere tiltak, eller at ansvarlige aksepterer denne risikoen.

4 FORBEDRINGSTILTAK NTNU

Basert på tilbakemeldingene fra ROS analysene og forslagene til tiltak fra Uninett har den rådgivende arbeidsgruppen følgende anbefalinger til konkrete tiltak for NTNU.

4.1 FORVALTNING

Det er i ROS-analyse pekt på noen svakhetspunkter rundt forvaltning av O365. Områdene dette gjelder er manglende forvaltning, rolleavklaringer og en exitstrategi.

Etablering av forvaltning

Det er etablert et forvaltningsteam for O365 på 3 personer fra forvaltningsseksjonen og lagt en plan for kompetansebygging for disse.

Det er i tillegg opprettet et "kjerneteam"(støtteteam) av andre personer med sentrale funksjoner og kompetanse rundt O365 i IT-avdeling

Dette er gjort med utgangspunkt i styrende dokument for O365. Det må forankres hos ledelsen at teamet er ansvarlig for forvaltning av O365

Rolleavklaring

Det må jobbes videre med å definere viktige roller i forhold til forvaltning.

Blant annet må NTNUs rolle som **behandlingssansvarlig** ovenfor Microsoft være tydeligere. Viktige roller som forvaltningsansvarlig (Systemeier) må defineres og beskrives.

Personvern og informasjonssikkerhet

Forvaltningsansvarlig (Systemeier) skal fortløpende vurdere informasjonssikkerheten i forhold til nye tjenester og systemløsninger. Noen av de viktigste områdene vil være:

- Ny norsk personvernlov (GDPR)
- Samkjøre forvaltningen med krav i **ISMS**

Exitstrategi:

Forvaltningsteam blir ansvarlig for å utarbeide en «overordnet exitstrategi» Dette innebærer blant annet:

- Jevnlig følge med i utviklingen for løsningen
- Vurdere kost/nytte jevnlig
- Jevnlig vurdere IT strategi i forhold til Plattformen
- Beskrive hovedaktivitetene som må gjøres ved en eventuell avslutting av tjenesten

4.2 OPPLÆRINGSTILTAK

Resultatene fra ROS analysene viser at mange av de høyeste risikoene går direkte på brukernes holdninger og feil/ikke ønsket bruk av løsningene. Dette gjelder både for løsninger i sky og on-premise. Feil bruk av epost i forhold til sensitive data og deling av innhold til feil mottakere er eksempler på dette.

Basert på tilbakemeldingene fra ROS analysene så anser gruppen det som svært viktig at NTNU tar tak i dette området på flere nivåer som adresserer både opplæringsbehov og generelle krav/holdninger:

- **Informasjon og kommunikasjonsarbeid**
    - Adressere holdninger og ønsket bruk av systemene
    - Utarbeide kommunikasjonsplan med ønsket informasjon. Informasjonssikkerhet skal være en viktig del.
    - Etablere og kommunisere god praksis for dokument og informasjonshåndtering ved NTNU
    - Synlig og tydelig informasjon lett tilgjengelig på Innsida og andre relevante kanaler
- **Tilbud om opplæring i ønsket bruk av skytjenestene.**
    - Klasseromskurs på ønsket bruk av skytjenestene hvor informasjonssikkerhet er en del av kurset.
    - Utnytte Læringsportalen som arena for e-læring og kursing.
- **Opplæring av NTNU IT.**
    - Med spesielt fokus på sikkerhetsmuligheter i Azure/O365
    - Informasjonssikkerhet i O365
- **Utvikle et e-læringskurs som går på informasjonssikkerhet i Office 365**
    - Bygge på «God praksis ved NTNU for lagring og dokument/informasjonsforvaltning»
    - Få inn informasjonssikkerhet som en del av Office 365 e-læringskurset som er utviklet for NTNU. Lenke
    - Vurdere om dette skal være obligatorisk for alle ansatte ved NTNU
- **Etablere en forståelse i organisasjonen for klassifisering av innhold «Åpent, Internt, fortrolig og strengt fortrolig»**
    - Informasjonsarbeid knyttet til dette.
        - Skal ivaretas av ISMS prosjektet.

4.3 RUTINER OG RETNINGSLINJER

Office365 er tett integrert mot datasystemer i egne datahaller og det meste av brukerutstyret i NTNU. Det er ikke bare snakk om enkeltprodukter, men en helt ny infrastrukturplatform. Det er derfor viktig at vi har rutiner og retningslinjer som ivaretar alle aspekter.

Det anbefales at Forvaltningsteam for Office 365 får ansvaret for å **påse** at det finnes og etterleves gode rutiner og retningslinjer omkring følgende hovedområder.

- **Brukeradministrasjon**
    - Ansatte i forskjellige kategorier
    - Studenter
    - Administratorer
- **Dataadministrasjon**
    - Databehandleravtaler
    - Dataeiere
    - beskyttelse av data (KIT), etc.
- **Forvaltning av tjenestene**
    - Økonomi
    - SLA
    - Hvilke tjenester skal vi benytte?
    - Påse at sourcingstrategi til NTNU etterfølges
- **Utvikling**
    - Retningslinjer for integrasjon
- **Sikkerhet**
    - Logging for å sikre KIT
    - Kontinuerlig tilpasse sikkerhetsnivå. MS lanserer nye tjenester her hver mnd.

  Listen er ikke uttømmende.

4.4 TEKNOLOGISKE FORBEDRINGSTILTAK OG OVERVÅKING

Microsoft leverer nye tjenester kontinuerlig, mange av disse gjør at sikkerheten blir bedre for hver dag som går, dersom man velger å ta de i bruk vel og merke. For å oppnå en tilfredsstillende sikkerhet der

man kan lagre og behandle både ÅPEN, INTERN og FORTROLIG informasjon så er det viktig å ha riktig lisensieringsnivå. Det er også viktig i forhold til konfidensialitet, tilgjengelighet og integritet.

Sikring av administrative tilganger

- Ta i bruk Azure AD PIM
- Etablere rutiner rundt forvaltning av administrative tilganger
- Etablere 2 faktor autentisering for administrative tilganger
- Logging av aktiviteter utført av administrative brukere

Utvide plattformen til å kunne håndtere fortrolig informasjon

- Aktivere tjenestene IRM/RMS i Tenant
    - Vurdere å involvere sektoren i dette arbeidet

Implementere klassifisering av innhold

- Det skal implementeres løsning for klassifisering av innhold på Office 365 plattform i henhold til føringer fra informasjonssikkerhet ved NTNU
    - Ref Policy for informasjonssikkerhet ved NTNU på innsida.
- Samkjøres med ISMS prosjektet.

Kost / Nytte vurdere Office 365 lisens opp mot funksjonalitet og sikkerhet

- Involvere lisenspartner og Microsoft til en gjennomgang
- Utarbeide en kost/nytte analyse for NTNU

Få på plass plan 2 SharePoint online som lisens i Office 365 Tenant for NTNU

- Dette gjør det mulig å etablere IRM/RMS funksjonalitet mm
- Skal være gratis ifølge Microsoft. Gjøres igjennom lisens for «Project online essentials faculty/students"

Etablere teknisk løsning for å kunne ta backup av relevante tjenester/løsninger i plattformen

- Det ansees ikke som nødvendig å etablere ekstern backupløsning for Office 365 som plattform.
- Det skal behovsvurderes igjennom ROS e.l hvorvidt hver enkelt løsning krever utvidet backup. Forvaltningsteam har et overordnet ansvar for å etablere løsning.
- Tiltak er iverksatt for å kjøre POC for å vurdere relevante leverandører på dette. Ole I. Langfeldt følger opp dette.

Etablere gode verktøy for drift/administrasjon av online tjenester

- Kjøre en POC på virtuelle maskiner i Azure som er tilknyttet NTNU Tenant for å se om dette gir raskere aksess til administrasjon av online tjenester via PowerShell etc.

NTNU