RAPPORT

Office 365 – God praksis for klassifisering og lagring av fortrolig informasjon

Målgruppe:	UH-Sektoren
Fra:	Snorre Jensen / Rune Myrhaug /Anette Osaland
Dato:	19.02.2018
Versjon:	1.0.1

Innhold

1 Forord

Bruken av skytjenester for lagring av dokumenter og annet innhold har eksplodert de siste årene og trenden er at innhold flyttes ut i skytjenester over hele verden. Dette påvirker sektoren i stor grad.

Moderne måter å samhandle på krever moderne beskyttelse. Tidligere var brannveggene og nettverkene samt de fysiske kontorplassene de viktigste barrierene for å komme til informasjon. Nå forventer brukerne at informasjon er tilgjengelig hele tiden fra overalt og på alle enheter. Virksomheter som velger å opprettholde de gamle tradisjonelle barrierene taper konkurransekraft mot de som følger med i tiden.

Gartner anerkjenner Microsoft 365 SharePoint og OneDrive som den ledende aktøren på skylagring og innholdsforvaltning. Tilnærmet hele UH-Sektoren i Norge har i større eller mindre grad adoptert plattformen inn i sin IT portefølje. Med investeringer på over $1 milliard årlig i «cybersikkerhet» og over 150 millioner brukere av Office 365 plattformen, er Microsoft helt avhengig av at plattformen er og forblir sikker.

UNINETT er og har vært en sterk pådriver på det å utarbeide god praksis for hvordan sektoren bør og kan ta i bruk skytjenester. Denne rapporten inngår i dette materialet med fokus på Office 365 plattformen og Azure. Rapporten er ment å være et verktøy for hele sektoren i forhold til det å gi tydelig veiledning i prefererte sikkerhetsbarrierer samt hvordan disse bør konfigureres for også å kunne håndtere fortrolig og strengt fortrolig informasjon.

1.1 Referanser

Referanse	Forklaring	Lenke
UH-Sky Startpakke Office 365	Veiledningsportal for skytjenester fra UNINETT	UH-Sky startpakke
Juridisk veileder for skytjenester	Anbefalinger og føringer fra UNINETT på skytjenester generelt	Juridisk veileder
UFS 136 - Veiledning i klassifisering av informasjon	God praksis for klassifisering av informasjon generelt	UFS-136
Forvaltningsdokument	Styrende dokument for Office 365 – god praksis for forvaltning av plattformen	Office 365 - forvaltning

Kapittel 5 og Appendiks kapittel 6.4 referer også i stor grad til hvilke lover og retningslinjer som rapporten har tatt utgangspunkt i for å utarbeide god praksis.

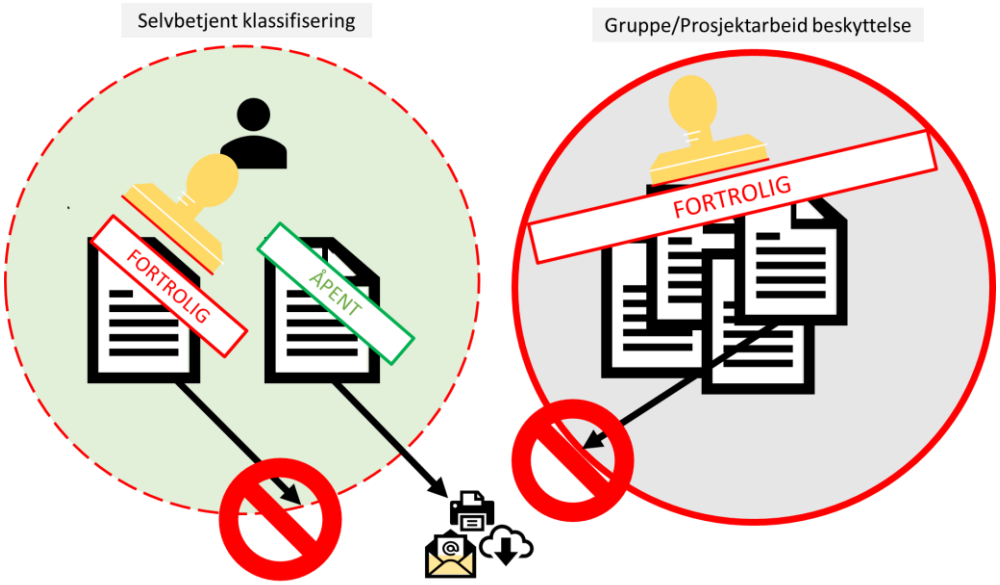
1.2 Sammendrag

Microsoft Office, OneDrive, SharePoint, Teams og Exchange online har blitt svært populære tjenester for både studenter og ansatte i sektoren. Parallelt med at bruken har tatt av i sektoren ser man at IT i stor grad har mistet kontroll over hvordan samhandling foregår og hvem som har tilgang til hvilke data.

UNINETT ser denne utviklingen og ønsker igjennom denne rapporten å gi noen gode råd i forhold til hvordan sektoren kan utnytte fordelene med moderne skytjenester og samhandling samtidig som man kan opprettholde nødvendige krav til konfidensialitet, integritet og sikkerhet.

En prosjektgruppe, se 2.1 «Prosjektgruppe for utarbeidelse av god praksis», ble satt sammen for å utarbeide god praksis for sektoren slik at studenter og ansatte på en enkel og trygg måte kan benytte skytjenestene til også å behandle informasjon av sensitiv art.

Resultatene fra prosjektgruppas arbeide er tydelige på at hver institusjon bør legge til rette for sikker samhandling i grupper/prosjekter, samt gjøre hver enkelt student/ansatt i stand til selv å klassifisere/sikre innhold. Dette kan oppnås igjennom en kombinasjon av god informasjon/ opplæring samt bruk av moderne teknologi. Denne rapporten beskriver anbefalt god praksis på disse områdene.



Prosjektgruppa har kommet frem til at «Azure Information Protection» som teknologi bør benyttes for å klassifisere og kryptere innhold i Office 365.

1.2.1 Klassifiseringsnivåer

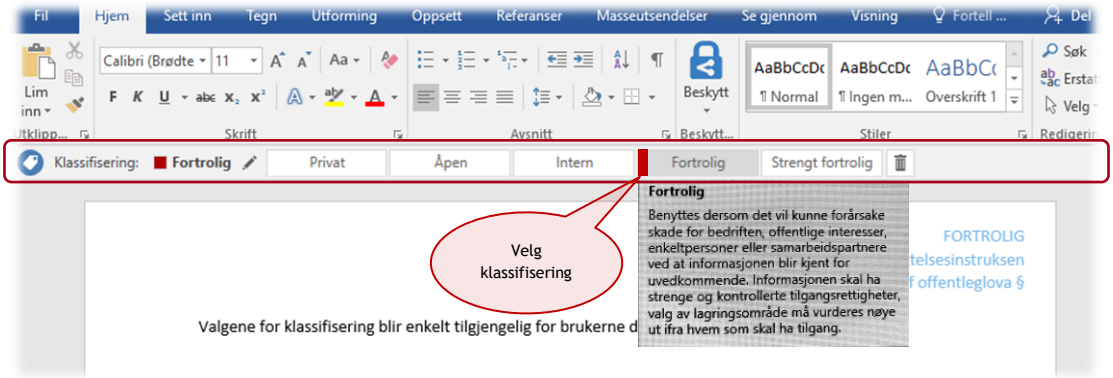
UNINETT veileder (UFS 136) for klassifisering av informasjon er lagt til grunn for god praksis i Office 365.

Figur 1- God praksis for klassifisering av innhold i sektoren.

Klassifiseringen Privat er lagt til av prosjektgruppen og ansees som relevant.

1.2.2 Selvbetjent klassifisering

«Slik ser det ut i Word for en bruker som blir gitt muligheten til selvbetjent klassifisering»



Figur 2 Selvbetjent klassifisering i Word

Beskyttelse bygges inn i dokumentene istedenfor stedet de lagres. Dette sikrer at barrierene respekteres uavhengig av hvem som får tilgang til dokumentene. Ved klassifisering av dokumentene til nivå «Fortrolig» eller «Strengt fortrolig» vil dokumentet bli beskyttet av AIP kryptering og tilganger styres enten av forfatteren eller fra dokumentbiblioteket.

Riktig oppsett av Office 365 og Mac/Windows setter brukerne selv i stand til enkelt å velge klassifisering. – Opplæring og informasjon i bruk blir viktig.

Denne barrieren vil kunne åpne for nye bruksområder og erstatte andre måter å behandle fortrolig informasjon på.

Prosjektgruppa er også tydelige på at det er gjort for lite funksjonell testing i bruken av denne teknologien i sektoren og ønsker at det skal gjennomføres en større pilot for å kvalitetssikre anbefalingene i denne rapporten. Piloten bør også utarbeide god praksis til sektoren med tanke på opplæring, informasjonsmateriell og rutiner som må endres som følge av dette. Dokumentenes livsløp må ivaretas og overføring til sak/arkiv er blant de momentene som må tenkes igjennom.

Prosjektgruppas vurdering av lovverket legger til grunn at behandling av fortrolig og strengt fortrolig informasjon kan gjøres i Office 365 (EU) så lenge nødvendige sikkerhetsbarrierer innføres. Se kapittel 5 for lovverk og ytterligere informasjon.

2 Bakgrunn

Som tidligere nevnt så er Office 365 adoptert av hele sektoren i større eller mindre grad. Plattformen med OneDrive, SharePoint online og Exchange online i spissen overtar i større og større grad informasjon som tidligere har blitt behandlet innenfor institusjonenes brannvegger og kontroll.

Den tilgjengeligheten og enkelheten i samhandling og deling av innhold som plattformen gir er på mange måter årsaken til suksessen. Men samtidig utgjør den en større risiko for både tilsiktet og utilsiktet spredning av informasjon som kan være skadelig for virksomheten og/eller enkeltpersoner.

Denne bekymringen er reell og skaper stor usikkerhet både i sektoren og samfunnet generelt. En stor andel av virksomhetene som utnytter skytjenestene har et bevisst forhold til det å ta det første steget ut i sky, men når først steget er tatt så ser man seg blind på alle de mulighetene for ekstra sikring som finnes uten å i praksis implementere disse.

Politihøgskolen kjører vinteren 2017/2018 et prosjekt med navn «Fra fil til sky» som innfører moderne samhandlingsarenaer hvor store deler av dokumentarbeidet for studenter og ansatte vil foregå i Office 365. OneDrive, Teams og SharePoint online er viktige arenaer der.
Det ble i dette prosjektet satt av midler til å utrede hvilke sikkerhetskomponenter fra Office 365 som vil kunne tilby den nødvendige tryggheten for at institusjonen skulle kunne behandle den samme informasjonen i sky som tidligere har ligget lagret på filservere innenfor institusjonens egne brannmurer.

Enable AS v/Snorre Jensen som leder dette prosjektet for Politihøgskolen tok initiativ til et møte med Microsoft v/Ole Tom Seierstad og andre nøkkelpersoner i sektoren som jobber med Office 365 og informasjonssikkerhet. Dette møtet ble avholdt under UNINETT-konferansen og sektoren stilte med representanter fra både NTNU, Nord og Politighøgskolen.

Resultatet fra dette møtet ble et prosjektmandat med fokus på å utarbeide en «God praksis for behandling av fortrolig/sensitiv informasjon i Office 365» for sektoren. En av forutsetningene var at UNINETT skulle delta i prosessen og eie resultatet.

UNINETT godkjente prosjektet i Januar 2018 og det ble avholdt et oppstartsmøte med relevante deltakere fra de respektive Universitet/Høgskolene for å sette sammen en prosjektgruppe med mandat til å jobbe frem forslag til god praksis for sektoren.

2.1 Prosjektgruppe for utarbeiding av god praksis

Med utgangspunkt i møtet på UNINETT-konferansen og forankring hos UNINETT ble det kjørt et oppstartsmøte med følgende institusjoner som hadde meldt sin interesse i å bidra inn i dette arbeidet:

- Politihøgskolen
- NTNU
- Nord Universitet
- Universitetet i Agder
- Microsoft / Enable AS
- UNINETT AS

Hver institusjon valgte ut to personer som skulle delta i kjerneteamet for prosjektet. Listen under inneholder kjerneteamet og hvilken institusjon de representerer.

Institusjon/Firma	Person	Epost	Rolle
UNINETT	Rune Myrhaug	rune.myrhaug@uninett.no	Bestiller
Enable AS	Snorre Jensen	snorre@enable.no	Prosjektleder
Nord Universitet	Per Gustav Gården	per.garden@nord.no	Prosjektdeltaker
NTNU	Per Atle Eliassen	per.atle.eliassen@ntnu.no	Prosjektdeltaker
Nord Universitet	Erik Gaukerud	erik.gaukerud@nord.no	Prosjektdeltaker
Politihøgskolen	Rikard Bye	rikard.bye@phs.no	Prosjektdeltaker
NTNU	Vebjørn Slyngstadli	vebjorn.slyngstadli@ntnu.no	Prosjektdeltaker
NTNU	Ole Ingvard Langfeldt	ole.langfeldt@ntnu.no	Prosjektdeltaker
Universitetet i Agder	Hans Erik Conrad Hansen	hans.e.hansen@uia.no	Prosjektdeltaker
Universitetet i Agder	Anette Thorkildsen Osaland	anette.osaland@uia.no	Prosjektdeltaker
Politihøgskolen	Bjørn Harald Rismoen	Bjorn.Harald.Rismoen@phs.no	Prosjektdeltaker
Microsoft	Siu Leung Cheung	slcheung@microsoft.com	Teknisk Fagperson
Microsoft	Christoffer Lokrheim	chrislok@microsoft.com	Løsningsarkitekt

Denne rapporten er i stor grad basert på resultatene etter tre arbeidssamlinger med prosjektgruppa og gjennomføring av «Proof of Concept» på nøkkelfunksjoner man ønsket å sjekke ut. Generelt god praksis fra andre virksomheters sikkerhetsarbeid og Microsoft ligger også til grunn for beslutningene og anbefalingene.

Gå til Appendiks 6.2 for innsikt i prosjektgruppas arbeidsmetodikk, samlinger og tema.

2.2 Resultater fra PoC testing av «God praksis»

I forbindelse med prosjektgruppas arbeid ble det etablert to adskilte testmiljøer hvor Nord Universitet og Politihøgskolen testet begge konseptene.

- Generell tilbakemelding fra POC testing er at prosjektgruppa har tro på dette for sektoren.
- IRM/AIP er godt egnet til samhandling på fortrolig informasjon, på tvers av flere institusjoner.

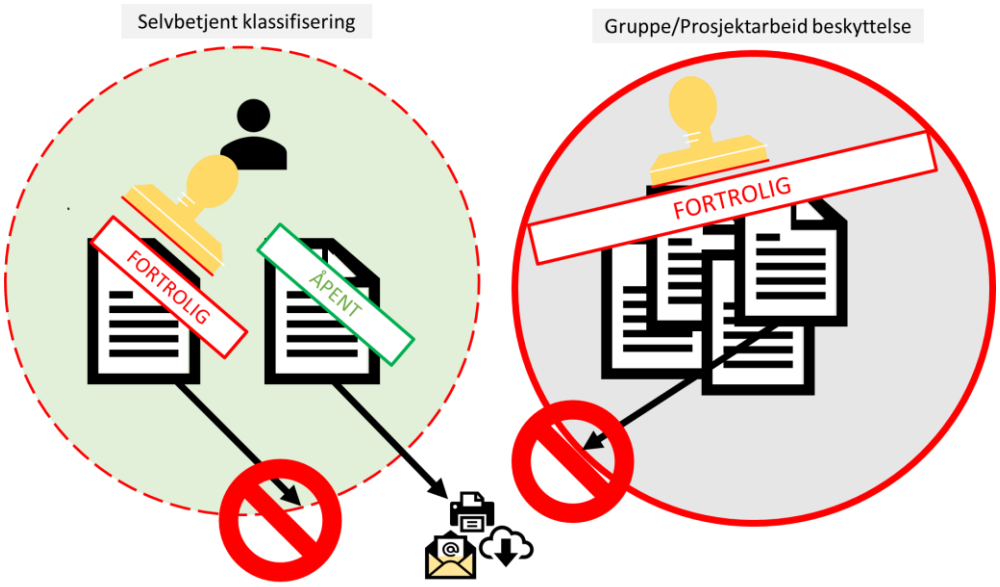
Følgende utfordringer ble identifisert igjennom testing og bør tenkes igjennom før implementering:

- Teams Klienten – umoden i forhold til behandling av IRM beskyttet informasjon
- IRM Beskyttede PDF dokumenter krever egen leser som støtter dette. Ikke alle PDF lesere støtter beskyttede dokumenter.
- Diverse utfordringer med eldre operativsystemer samt Office versjoner. Før «utrulling» ved institusjonene må de administrerte devicene/pcene testes og kanskje tilpasses noe.
- Det er ikke fullverdig funksjonalitet for behandling av IRM/AIP beskyttet dokumenter i nettleseren - Office Online.
- Per februar/mars 2018, se Appendiks 6.8 "Roadmap / hva kommer / dagens begrensninger", bør en ved å ta i bruk Azure Information Protection (AIP) være klar over at AIP support i Mac OS kan være noe begrenset.

3 Funksjonelle behov i sektoren

Prosjektgruppen har prioritert å jobbe med to typer bruksscenario som i stor grad dekker behovene i institusjonene for behandling av fortrolig/strengt fortrolig informasjon:

- **Selvbetjent klassifisering**: Det å gi den enkelte medarbeider mulighetene til selv å klassifisere informasjon som fortrolig/strengt fortrolig. Enten forankret i lovverket eller på eget initiativ.
    - Fortrolig informasjon blir automatisk kryptert og beskyttet uavhengig av plassering.
- **Gruppe/Prosjektarbeid:** Sikre beskyttelse av dokumenter/samhandlingsarenaer i Office 365 hvor flere mennesker skal jobbe med informasjon som faller under klassifiseringen fortrolig/strengt fortrolig.
    - Sikkerhet bygges inn i «Samhandlingsrommet» og kan ikke oppheves av deltakerne.



3.1 Trusler og behov for beskyttelse

Det vanlige i offentlig sektor har gjerne vært å ha egne sikre soner for behandling av data klassifisert som fortrolig og strengt fortrolig. Sperrene har da vært implementert i form av brannvegger og beskyttede nettverk. Med riktig utnyttelse og bruk vil AIP/dokumentbeskyttelse utgjøre en moderne versjon av denne barrieren og erstatte enkelte slike systemer.

Det er fort gjort å tenke "fremmede makter" når en snakker om behov for å beskytte fortrolig informasjon, men i de fleste tilfeller er det utro tjenere (egne ansatte/studenter) eller "objekt" (personer/bedrifter/institusjoner) som står institusjonen nær som har interesse i å tilegne seg slik informasjon.

Ved å flytte fortrolig informasjon ut av eget datasenter vil dette i seg selv kunne gjøre det vanskeligere for nærliggende "objekt" å tilegne seg fortrolig informasjon. Dette fordi de som har interesse av å tilegne seg informasjonen hverken vil ha fysisk tilgang (lagring & nettverk) til der data er lagret eller noen mulighet til å overstyre det logiske laget av sikkerhetsbarrieren (prosesser og rutiner).

3.2 Selvbetjent klassifisering

Et av de viktigste behovene som prosjektgruppa har avdekket er det å sette enkeltpersoner i stand til selv å klassifisere informasjon på en enkel og forståelig måte som er uniform for sektoren og som ikke er avhengig av hvor informasjonen lagres og sendes.

Prosjektgruppa har kommet frem til at «Azure Information Protection» som teknologi bør benyttes for å klassifisere og kryptere innhold i Office 365.

Generelt gjelder det at informasjonsutsteder skal, på forhånd, vurdere skadepotensiale dersom uvedkommende får tilgang til informasjonen, og på bakgrunn av dette beskytte informasjon iht. til aktuell klassifisering.

3.3 Gruppe / Prosjektarbeid beskyttelse

Det andre tydelige behovet som er identifisert er når grupper av mennesker skal jobbe sammen om innhold som er- eller skal klassifiseres som fortrolig og/eller strengt fortrolig.
Eksempler på dette kan være forskningsprosjekter, helsedata eller sensitiv personinformasjon.

Det viktigste i denne sammenhengen er at det skal **ikke** være opp til enkeltpersoner i en slik gruppe å selvstendig vurdere behovet for beskyttelse. Eieren av innholdet/prosjektet tildeles normalt et slikt ansvar eller det bør etableres forvaltning omkring slike samhandlingsarenaer ved institusjonen. IT kan naturlig tildeles et slikt forvaltningsansvar.

Prosjektgruppa har kommet frem til at «IRM i Office 365» som teknologi bør benyttes for å kryptere innhold i dokumentbiblioteker med fortrolig eller strengere innhold.

4 Anbefalt «god praksis» for sektoren

Office 365 er en plattform med mange forskjellige arenaer for samhandling. Det er prosjektgruppas anbefaling at «ut av boksen» funksjonalitet i Office 365 kan benyttes til all informasjon som faller inn under klassifiseringen «Åpent» og «Internt». ROS-vurdering ved innføring bør allikevel gjennomføres.

Tjenesteforvaltning handler om hvordan en tjeneste eller en plattform skal implementeres, driftes og videreutvikles etter at den er innført og tatt i bruk i organisasjonen. En forvaltningsplan bør utarbeides for alle større IKT-systemer som griper inn i virksomhetens arbeidsprosesser og som har avgjørende betydning for virksomhetens primærproduksjon. Forvaltningsplanen bør ha klare linjer til det etablerte regimet for generell IT-drift, gjerne basert på ITIL-rammeverket.

For Office 365 er behovet for en forvaltningsplan ekstra stort, ettersom O365 består av et stort antall moduler som til en viss grad henger sammen, men som man nødvendigvis ikke trenger å ta i bruk samtidig. Her gjelder det å ha en klar plan for hvilke tjenester/moduler som skal benyttes av ulike brukergrupper i organisasjonen, og hvordan disse tjenestene/modulene skal benyttes. Når denne planen foreligger og er beskrevet, starter den kontinuerlige jobben med å utnytte systemet best mulig, og videreutvikle systemet med den hensikt at det skal bidra til å understøtte kjernevirksomheten.

Les mer om forvaltning her http://startpakke.uhsky.no/docs/saas/office365/kap4/ , med link til NTNU sin mal for forvaltning.

Det er prosjektgruppens intensjon at dette dokumentet skal benyttes som grunnlag for en større «pilot» på praktisk innføring av denne funksjonaliteten ved en av institusjonene i sektoren. Dokumentet skal være gjenstand for revisjon etter evaluering av en slik pilot.

4.1 Prosess ved implementering av klassifisering i institusjonen

Behandling av fortrolig informasjon utgjør en liten andel av det totale behov for lagring og deling av informasjon. Erfaringstall fra andre bransjer tilsier at ca. 5 % av informasjonen som behandles kan ansees å falle under klassifisering fortrolig eller strengere. For å implementere lagring og deling av fortrolig informasjon i Office 365 på best mulig måte vil det være en god praksis å identifisere personer/grupper/prosjekter som en vet behandler fortrolig informasjon, slik at en kan rette informasjon og opplæring til disse målgruppene.

Målrettet opplæring og tydelig informasjonsmateriell vil være viktig – både til ansatte som skal behandle fortrolig informasjon og IT-ansatte som skal hjelpe til med oppsett.

Praktisk bruk av klassifisering må forankres i hver enkelt institusjon. Institusjonene er selv ansvarlig for å utarbeide interne retningslinjer, samt opplæring av egne ansatte/studenter. I tillegg må en påse at AIP/IRM oppsett, samt de interne retningslinjene, er i samsvar med institusjonens akseptkriterier.

Særlig i de tilfeller der det behandles en mengde fortrolig informasjon samlet i SharePoint dokumentbibliotek vil det være en god praksis å kjøre en selvstendig ROS-analyse/verdivurdering.

Det er også viktig når man utarbeider rutiner og god praksis for institusjonen at man ivaretar livsløpet til dokumentene og sikrer at informasjon som er klassifisert som fortrolig blir ivaretatt i forbindelse med eventuell overføring til sak/arkivsystemer etc. Sannsynligvis bør dokumentene «avklassifiseres» eller krypteringsbeskyttelse bør fjernes.

Det er også viktig å tenke på at innhold som klassifiseres som fortrolig/strengt fortrolig på ett tidspunkt, ikke nødvendigvis er det på et senere tidspunkt.

Det er et ledelsesansvar å formidle tillit til skytjenester / Office 365. Det eksisterer mye tvil og usikkerhet ute i de forskjellige miljøene omkring sikkerhet etc.

Tydelig kommunikasjon om god praksis og ønsket bruk av tjenestene bør forankres i ledelsen.

4.2 Hensyn å ta ved implementering

Når en oppretter en tenant fra Norge, vil tenant'en automatisk bli tagget "EU". For Office 365 moduler som er EU-kompatible vil data bli lagret innad i EU. Dette gjelder blant annet OneDrive for Business, SharePoint og Exchange Online. Ikke alle moduler er EU-kompatible, dette gjelder spesielt nye moduler i Office 365. For en liste over hvilke moduler som er EU-kompatibel, se: http://o365datacentermap.azurewebsites.net

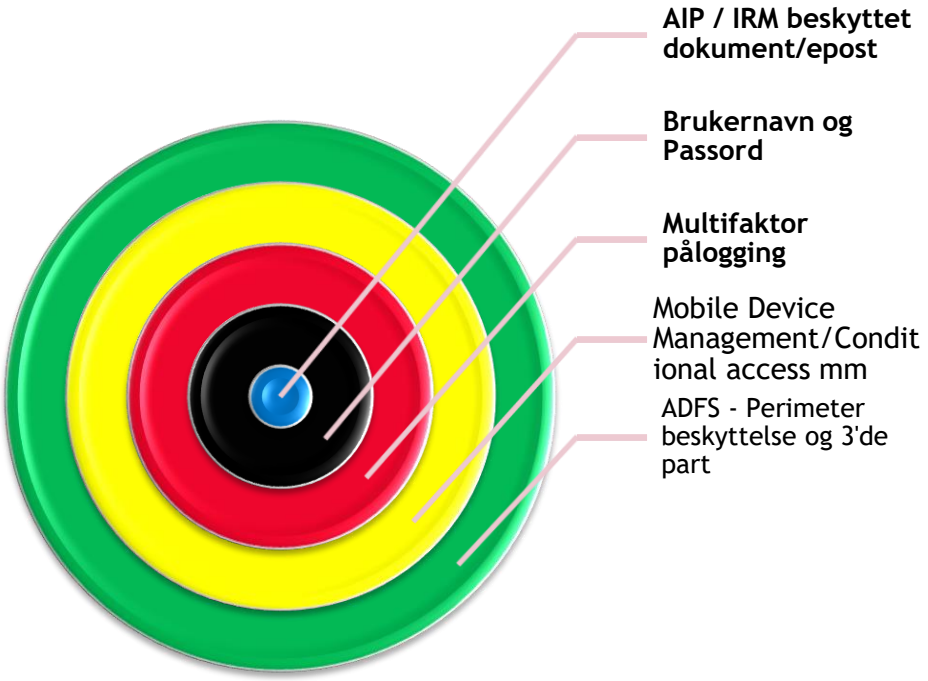
Se også kapittel 2.2 "Resultater fra POC testing" for øvrige momenter som bør tas hensyn til ved implementering.

4.3 Viktige sikkerhetsbarrierer

Office 365 og Azure er en kompleks og stor plattform med svært mange muligheter til å justere sikkerhetsbarrierer. Prosjektgruppa har evaluert disse og sett på god praksis hos andre.

Prosjektgruppa anbefaler bruk av AIP og IRM «Information Rights Management» for dokument/epost beskyttelse ved behandling av fortrolig informasjon i Office 365.

Øvrige barrierer som hever sikkerheten ytterligere vurderes opp mot brukervennlighet og kostnader av den enkelte institusjon.



Figur 3. Barrierer i Office 365

AIP og IRM beskyttelse av dokumenter og epost sikrer at de barrierene som legges på også beholdes selv om informasjonen lagres/sendes ut av institusjonens kontroll.

Dokumenter som beskyttes med IRM / AIP og krypteres ivaretar følgende viktige sikkerhetsargumenter

- Kun de som er gitt tillatelser til dokumentet/epost får åpnet det
- Personer som bytter rolle / slutter e.l - mister tilgangen automatisk
- Dokumenter som kommer på avveie beskyttes fortsatt av de barrierene som til enhver tid gjelder

Verktøykassen i Office 365/Azure inneholder flere barrierer som kan være relevante i forhold til ytterligere sikring av digitalt innhold. Det er også viktig å påpeke at AIP/IRM kun beskytter epost og Microsoft Office dokumenter. PDF dokumenter kan også beskyttes, men gir noen utfordringer. Se Appendiks "Kompatible filtyper" for detaljer på filtyper og beskyttelse.

Se også Appendiks 6.5 "Verktøykassen (barrierer)" for mer informasjon.

Prosjektgruppen har kommet frem til at følgende barrierer bør implementeres som ett minimum.

Teknisk barriere	Åpent	Internt	Fortrolig	Strengt fortrolig
Brukernavn /Passord	Nei	Ja	Ja	Ja
Multifaktor autentisering Azure AD	Nei	Nei	Ja	Ja
Kryptering – Cloud key (IRM/AIP)	Nei	Nei	Ja	Ja
Kryptering – Hold your own key (HYOK) / Office 365 Customer key *	Nei	Nei	Nei	Vurderes selvstendig
Conditional Access **	Nei	Nei	Vurderes selvstendig	Ja
Lockbox *	Vurderes selvstendig	Vurderes selvstendig	Vurderes selvstendig	Vurderes selvstendig

*) Krever ekstra lisensiering utover A3
**) For avansert "Conditional Access" kreves ekstra lisensiering utover A3

Standard lisensavtale med Crayon gir A1 lisens. Det betyr at det vil være en kostnad med å få selvbetjent klassifisering (AIP), som en får i A3. Alternativ til å kjøpe en A3 lisens er å kjøpe EMS E3 lisenser for å få samme sikkerhetsfunksjonalitet.

Dette trenger kun å anskaffes for brukergrupper som behandler fortrolig informasjon.

Se kapittel 6.6 for detaljer omkring lisensiering

Barrierer beskrevet i denne rapporten omhandler "Data laget". I tillegg er datasentrene Office 365 kjører på meget godt sikret, en "Fysisk sikkerhet" som det skal mye ressurser til for å overgå. På det logiske sikkerhetslaget er det implementert flere prosesser og rutiner som sørger for sikkerhet. Les mer om dette her: http://download.microsoft.com/download/6/6/2/662F89E4-9340-4DDE-B28E-D1643681ADEB/Security%20in%20Office%20365%20Whitepaper.docx

4.4 God praksis «Selvbetjent klassifisering»

Det er god praksis å ta utgangspunkt i UNINETT sin veileder for klassifisering av innhold og prosjektgruppa har basert seg på denne. Denne skal også brukes for å etablere forståelse i egen organisasjon for hvilke informasjonselementer som vil falle under de respektive klassifiseringene.

- Lenke: https://www.uninett.no/infosikkerhet/klassifisering-av-informasjon

Følgende punkter er også å betrakte som god praksis for institusjonene:

- Azure Information Protection klientutrulling. Styrt utrulling av og oppdatering av denne på administrerte maskiner ved institusjonen.
- God informasjon / opplæring av brukergruppene som skal kunne håndtere/forvalte fortrolig informasjon.
- For at sikring og klassifisering av innhold skal kunne fungere for en institusjon er et viktig at det skapes forståelse og aksept for innføringen. Oppsett av Azure Information Protection i institusjonenes Office 365 Tenants ihht føringene i denne rapporten.
- Det er viktig at policyene for god praksis implementeres teknologisk så snart som mulig. Funksjonaliteten er allerede tilgjengelig for brukerne ut av boksen og da med feil definisjoner/navngiving på klassifisering og muligheter i forhold til god praksis.

Se Appendiks 6.1 «**Teknisk implementering av Azure Information Protection**» for detaljert anbefaling på hvordan sette opp Globale Policyer i AIP for den enkelte institusjon.

4.5 God praksis «Prosjekter / Dokumentbiblioteker»

Bruken av IRM (Information Rights Management) med bruk av RMS (Rights Management Service) er den anbefalte måten å sikre fortrolig og strengt fortrolig informasjon som en gruppe av mennesker skal ha tilgang til. Typiske eksempler på dette er prosjekter hvor en ROS analyse peker på at fortrolig informasjon skal behandles, eller det er tvil om at innholdet er og vil være av en art som faller inn under denne klassifiseringen.

Prosjektgruppa har kommet frem til at teknologien som anbefales brukt for å gi denne typen beskyttelse er «Information Rights Management» også benevnt som IRM/RMS. Dette er en tjeneste som baserer seg på Azure Information Protection, men er primært rettet mot SharePoint og dokumentbiblioteker.

Egen ROS-vurdering bør legges til grunn om det eksisterer usikkerhet om klassifisering og sårbarhet i de dataene som skal behandles.

- Det er god praksis å ha en egen SharePoint SiteCollection på SharePoint siter som inneholder fortrolige dokumenter. Ved opprettelse av en "Office 365 gruppe" vil automatisk en egen SiteCollection bli laget.
- IRM aktiveres på dokumentbibliotek-nivå. Det er god praksis å lage ett eget dokumentbibliotek, "Fortrolige dokumenter", som IRM aktiveres på.
- Det anbefales videre å ta en gjennomgang av sikkerhetsinnstillingene på dokumentbiblioteket, for å for eksempel hindre at visitors/gjester har tilgang til dette dokumentbiblioteket.
- Det er også anbefalt å ta en gjennomgang av innstillingene for aktivitets-logging. Dette gjøres på SiteCollection-nivå.

4.6 Microsoft Exchange online / on-premise og Hybrid

Prosjektgruppa og denne rapporten adresserer i liten grad sikring av epost og god praksis for det i sektoren. Her må det kjøres et eget prosjekt for å utarbeide god praksis for dette. Det er for mange usikkerheter knyttet til konsekvenser ved hybridmiljø og kommunikasjon på tvers i sektoren til at prosjektgruppa kan anbefale en god praksis for dette.

Fortrolig informasjon bør på generelt grunnlag ikke sendes per epost. Det finnes dog teknologi i Office 365 som gjør at en kan håndtere fortrolige eposter. Azure Information Protection for Exchange Online og SMIME er eksempler på teknologier som kan benyttes.

Se Appendiks "Verktøykassen (Barrierer)" for mer informasjon.

Prosjektgruppa oppfordrer UNINETT til å kjøre en egen aktivitet på dette området med formål om å etablere en god praksis for hele sektoren.

5 Lovverk og føringer

Hvordan opplysninger skal håndteres/sikres avhenger ikke bare av hvilke typer/klasser opplysninger det dreier seg om, for eksempel alminnelige eller sensitive personopplysninger (som er typene/klassene vi finner i personvernlovgivningen). Mengden opplysninger (volum), hvem opplysningene gjelder (for eksempel barn, ungdom, voksne, osv.) og antall personer som opplysningene relaterer seg til (mange, få, osv.) har også stor betydning. Det kan derfor bli for enkelt å bare typebestemme/klassifisere opplysningene i henhold til UFS 136 for å avgjøre hvordan de skal håndteres/sikres.

Konfidensialitet & Integritet:

- Konfidensialitet handler om at ingen skal ha tilgang til informasjon uten tjenestelige behov. Hindre at uvedkommende får tilgang til konfidensiell eller sensitiv informasjon.
- Integritet handler om at informasjon og systemer skal være korrekte og pålitelige. Hindre uønsket endring, sletting eller manipulering av informasjon.

Konfidensialitet og integritet må sees i sammenheng med hverandre når en beslutter hvordan opplysninger skal håndteres.

Se Juridisk veileder for skytjenester

5.1.1 Backup & Logging:

Prosjektgruppen har hatt fokus på "behov for beskyttelse" sett i forhold til klassifisering og behov for kryptering/barrierer for å få tilgang til informasjon. Regulatoriske krav som omhandler backup/restore og logging er ikke en del av det prosjektgruppen har undersøkt.

Office 365 har funksjonalitet som dekker logging (audit), backup/restore, DLP (Data Loss Prevention) se Appendiks 6.9 "Backup/restore, logging, DLP ".

I forbindelse med ROS-analyse, ved innføring av Office 365, bør det gjøres en vurdering av om den innebygde restore muligheten i Office 365 er god nok. Det finnes 3-parts verktøy dersom svaret er nei. Se: https://www.uninett.no/veileder-back-og-storage-service-0

5.1.2 Databehandleravtale Microsoft Office 365

For norske Office 365 tenanter, i UH-sektoren, ligger det alltid til grunn en databehandleravtale som sikrer OneDrive for Business, SharePoint og Exchange Online datalagring innad i EU.
Dette er en direkte avtale mellom Microsoft og den enkelte institusjon og kan til enhver tid hentes ut fra Administrasjonssidene for Office 365.

5.1.3 Datalagring utenfor Norge

Informasjon som går inn under sikkerhetsloven, med sikkerhetsgraderingene "Begrenset", "konfidensielt", "hemmelig" eller "Strengt hemmelig", er ikke en del av det prosjektgruppen har vurdert i forhold til datalagring utenfor Norge.

Prosjektgruppen har ikke på generelt grunnlag greid å identifisere noe fortrolig informasjon (dekket av UFS136) som per lovverk ikke kan lagres i Office 365 (Innad i EU, som gjeldende for norsk UH-sektor). Følgende lover, som omhandler arkiv og regnskap, må tas hensyn til:

- I henhold til bokføringsloven § 13 annet ledd, skal som hovedregel regnskapsmaterialet oppbevares i Norge.
- Arkivloven – krever at arkivverdig informasjon lagres i egne systemer i Norge. Det betyr ikke at dataene ikke også kan ligge i og produseres i Office 365.

Noen relevante linker som omhandler datalagring utenfor Norge:

- https://www.anskaffelser.no/skytjenester-cloud/lagre-og-behandle-data/personopplysninger-og-helseinformasjon-ved-en-skytjeneste
- https://www.arkivverket.no/for-arkiveiere/arkivering/skytenester
- https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet/normen/veileder-i-bruk-av-skytjenester-til-behandling-av-helse-og-personopplysninger
- http://www.ks.no/globalassets/endelig-rapport-om-bruk-av-skytjenester-i-kommunal-sektor.pdf

Se Appendiks 6.4 "Lovverk og føringer" for mere informasjon som prosjektgruppen mener er relevant i forhold til lovverket, samt Juridisk veileder for skytjenester.

5.1.4 Personvernforordningen – GDPR

Definisjon av personopplysninger: - Fra Datatilsynet.
https://www.datatilsynet.no/om-personvern/personopplysninger/

Det vil være en god praksis å behandle det meste av personopplysninger klassifisert som "Internt", samt sensitive personopplysninger klassifisert som "Fortrolig". Slikt som fødselsnummer bør behandles med aktsomhet selv om dette etter datatilsynets definisjon ikke inngår i sensitive personopplysninger.

Gjennom databehandleravtalen som norsk UH-sektor har på Office 365 forplikter Microsoft seg til å være "GDPR Compliant", men det er institusjonene sitt ansvar å overholde dette.

Microsoft har utarbeidet gode veiledere på hvordan plattformen kan og bør tilpasses for å understøtte den nye personvernforordningen i EU.
https://www.microsoft.com/en-us/TrustCenter/Privacy/gdpr/default.aspx

6 Appendiks

6.1 Teknisk implementering av Azure Information Protection

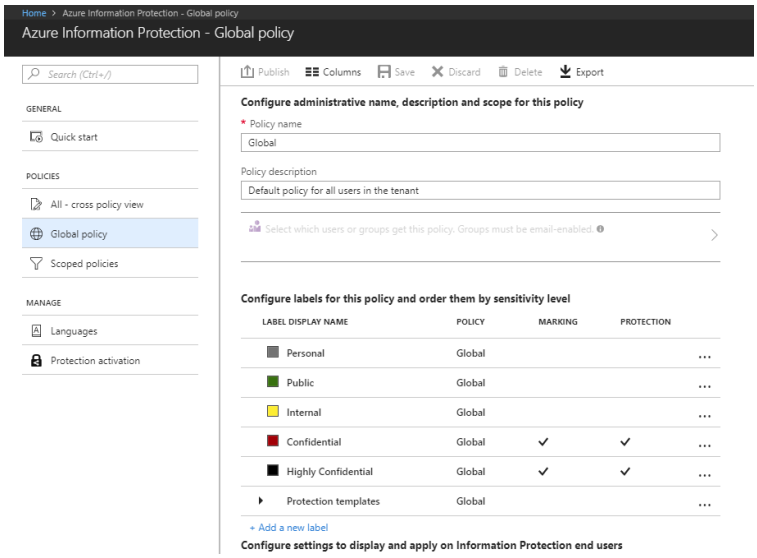
God praksis på klassifisering og navngiving for UH-Sektoren er i stor grad basert på de anbefalingene som Microsoft kommer med som «ut av boksen» standardinnstillinger og er gjeldende for alle som tar plattformen i bruk uten å gjøre endringer.

Forslagene til god praksis for sektoren har noen små forslag til forbedringer/tilpasninger for primært å sikre en uniform bruk av begreper knyttet til informasjonssikkerhet og klassifisering i sektoren for øvrig.

6.1.1 AIP konfigurasjon

https://docs.microsoft.com/en-us/information-protection/deploy-use/configure-policy

Logg på med Global Tenant Admin: https://portal.azure.com



6.1.2 Språkstøtte

Det anbefales å definere riktige engelske «Labels» før export/import norsk språkfil.
Følgende artikkel benyttes for å sikre korrekt innføring av språkstøtte i Azure Information Protection.
https://docs.microsoft.com/en-us/information-protection/deploy-use/configure-policy-languages

6.1.3 Engelske tekster og beskrivelser på klassifiseringene

Navnene under skal gjenspeile «God praksis i sektoren»
Klassifisering: **Personal**
Farge: Grå
Beskyttelse/kryptering: Ingen
Header/Footer/Watermark: Ingen
Text "Non-business information, for personal use only."

Klassifisering:**Public**
Farge: Grønn
Beskyttelse/Kryptering: Ingen
Header/Footer/Watermark: Ingen
Text "The information can be available to everyone and can be shared both internally and externally."

Klassifisering: **Internal**
Farge: Gul
Beskyttelse/kryptering – Ingen
Header/Footer/Watermark: Ingen
Text: "Information that requires protection and must have controlled access rights, storage platform must be evaluated based on who needs access to the information. This may be all students/employees or a group/department. Used in internal administrative procedure or if the information is not to be disclosed to unauthorized persons. Can be shared after assessment and need."

Klassifisering: Confidential
Farve: Rød
Beskyttelse/kryptering: Azure (Cloud key)
Tillatelse « »
Header/Footer/Watermark:
Text:"Classification should be used if it could cause damage to the company, public interests, individuals or collaborators that the information becomes known to unauthorized persons. The information should have strict access rights, the choice of storage platform must be considered carefully based on who needs access to the information"

Klassifisering: Highly Confidential
Farve: Sort
Beskyttelse/kryptering: Azure (Cloud key)
Tillatelse: « »
Header/Footer/Watermark: «…»
Text: "Classification should be used if it could cause significant damage to the company, public interests, individuals or collaborators that the information becomes known to unauthorized persons. The information should have the strictest access rights"

6.1.4 Norske tekster og beskrivelser på klassifiseringene

Klassifisering: **Privat**
Tekst «Ikke-virksomhetsinformasjon, kun til privat bruk.»

Klassifisering: **Åpen**
Tekst: «Informasjonen kan være tilgjengelig for alle og kan deles både internt og eksternt.»

Klassifisering: **Intern**
Tekst: «Informasjonen trenger beskyttelse og må ha kontrollerte tilgangsrettigheter. Valg av lagringsområde må vurderes ut ifra hvem som skal ha tilgang. Dette kan være alle studenter/ansatte eller en spesiell gruppe/avdeling. Benyttes ved intern saksbehandling eller dersom informasjonen ikke skal gjøres kjent for uvedkommende. Kan deles etter vurdering og behov»

Klassifisering: **Fortrolig:**
Tekst: «Benyttes dersom det vil kunne forårsake skade for institusjonen, offentlige interesser, enkeltpersoner eller samarbeidspartnere ved at informasjonen blir kjent for uvedkommende. Informasjonen skal ha strenge og kontrollerte tilgangsrettigheter, valg av lagringsområde må vurderes nøye ut ifra hvem som skal ha tilgang»

Klassifisering: **Strengt fortrolig**
Tekst: «Benyttes dersom det vil kunne forårsake betydelig skade for institusjonen, offentlige interesser, enkeltpersoner eller samarbeidspartnere ved at informasjonen blir kjent for uvedkommende. Informasjonen skal ha de strengeste tilgangsrettighetene»

6.2 Arbeidssamlinger prosjektgruppen

Det har blitt gjennomført 3 arbeidssamlinger i prosjektperioden for utarbeiding av god praksis for fortrolig / strengt fortrolig informasjon i Office 365.

Ta kontakt med prosjektleder Snorre Jensen /Enable AS for eventuelle detaljer i dette arbeidet:

6.2.1 Arbeidssamling 1.

- Microsoft v/Siu Leung Cheung gjennomførte en times teknologisk gjennomgang av alternative sikkerhetsmekanismer som finnes i Office 365/Azure.
- Felles diskusjon omkring hvilke teknologier gruppa ønsket å se nærmere på og kjøre testing omkring.
- Felles enighet om krav til POC «Proof of Concept» testmiljø og hvilke bruksscenarioer som skulle etableres for testing/kvalitetssikring
- Enighet i gruppa om å fokusere på to områder
    - Selvbetjent Klassifisering av innhold basert på AIP
    - Gruppe/prosjektarbeid – beskyttelse av dokumentbibliotek med bruk av tjenesten.
- Universitetet i Agder to ansvaret for å bistå i etablering av POC for AIP – Klassifisering
- Politihøgskolen tok ansvar for å «Hoste» POC miljø for IRM/RMS – Rights Management tjenesten for beskyttelse av dokumentbibliotek

6.2.2 Arbeidssamling 2

- Felles gjennomgang av POC testmiljøer.
    - UiA – på klassifisering av innhold.
        - Anette T. Osaland og Hans Erik Conrad Hansen hadde jobbet frem forslag på god praksis basert på Uninett klassifisering
    - Politighøgskolen – IRM/RMS – beskyttelse av Dokumentbiblioteker/SiteCollection.
        - Bjørn Harald Rismoen hadde etablert POC – testmiljø for beskyttelse av dokumenter knyttet til et «samhandlingsrom/prosjektrom»
- Gjennomgang av testplaner og tilbakemeldingsskjema for hver institusjon.
    - Samtlige deltakere oppfordret til å bistå aktivt i testing
- Videre diskusjon omkring forslag til «God praksis» og hva gruppa hadde tro på for sektoren

6.2.3 Arbeidssamling 3

- *Resultater fra testing gjennomgang.*
    - *Alle presenterte sine kommentarer og resultater.*
- *Grov gjennomgang av utkast til rapport og forslag til endringer før rapporten skal sendes på høring.*
- *Videre fremdrift og fordeling av ansvar.*

6.3 Microsoft Security – Relevante lenker

En samling av relevante lenker som Microsoft har bidratt med i prosjektet.

Det viktigste området som samler det meste Microsoft har omkring sikkerhet og personvern i sky.
https://www.microsoft.com/en-us/trustcenter/security/default.aspx

Design and operational security:
https://www.microsoft.com/en-us/trustcenter/security/designopsecurity

Network security:
https://www.microsoft.com/en-us/trustcenter/security/networksecurity

Encryption
https://www.microsoft.com/en-us/trustcenter/security/encryption

https://support.office.com/en-us/article/Configure-your-Office-365-tenant-for-increased-security-8d274fe3-db51-4107-ba64-865e7155b355

https://docs.microsoft.com/nb-no/microsoft-365/enterprise/microsoft-365-policies-configurations

https://docs.microsoft.com/nb-no/microsoft-365/enterprise/identity-access-policies

https://docs.microsoft.com/nb-no/microsoft-365/enterprise/secure-email-recommended-policies

https://docs.microsoft.com/nb-no/microsoft-365/enterprise/sharepoint-file-access-policies

6.4 Lovverk og føringer

6.4.1 UFS og veileder fra UNINETT

6.4.1.1 UFS136

https://www.uninett.no/infosikkerhet/klassifisering-av-informasjon

6.4.1.2 Veileder skytjenester

https://www.uninett.no/skytjenester/juridisk-veileder-skytjenester

6.4.2 Lov om forebyggende sikkerhetstjeneste (Sikkerhetsloven)

Sikkerhetsloven med forskrifter angir minimumskravene for beskyttelse av informasjon og objekter av betydning for rikets eller alliertes sikkerhet eller andre vitale nasjonale sikkerhetsinteresser.

Alle som skal behandle eller ha tilgang til sikkerhetsgradert informasjon er pliktig til å sette seg inn i sikkerhetsloven samt dennes forskrifter.

NB! Før sikkerhetsgradert informasjon kan behandles, lagres eller transporteres i et informasjonssystem, skal Nasjonal sikkerhetsmyndighet (NSM), eller den NSM bemyndiger, godkjenne systemet for angjeldende sikkerhetsgrad.

NSM er sertifiseringsmyndighet for informasjonssystemer som skal håndtere denne type informasjon.

Person som skal gis tilgang til informasjon gradert BEGRENSET, skal autoriseres.
Person som skal autoriseres for tilgang til informasjon gradert KONFIDENSIELT eller høyere, skal på forhånd sikkerhetsklareres (sikkerhetsloven kapittel 6).

Sikkerhetsloven
https://lovdata.no/dokument/NL/lov/1998-03-20-10?q=sikkerhetsloven
https://no.wikipedia.org/wiki/Sikkerhetsloven

Hjemmelsregister
https://lovdata.no/referanse/hjemmel?dokID=NL/lov/1998-03-20-10

Forskrift om informasjonssikkerhet
https://lovdata.no/dokument/SF/forskrift/2001-07-01-744/%C2%A7amp%3B#%C2%A7amp;

Forskrift om personellsikkerhet
https://lovdata.no/dokument/SF/forskrift/2001-06-29-722?q=personellsikkerhet

Veiledninger fra Nasjonal Sikkerhetsmyndighet
https://nsm.stat.no/publikasjoner/regelverk/veiledninger/

6.4.3 Beskyttelsesinstruksen

Kommer til anvendelse ved behandling av informasjon som trenger beskyttelse av andre grunner enn de som er nevnt i sikkerhetsloven med forskrifter. Instruksen gir bestemmelser om beskyttelse av informasjon og gjelder for statsforvaltningen.

For å kunne beskytte opplysninger etter denne instruksen må opplysningene kunne unntas offentlighet etter offentlighetslovens unntaksbestemmelser.

§ 3: « Gradering av et dokument skal bare foretas når det kan unntas offentlighet i medhold av offentlighetsloven og skadevirkninger som nevnt i § 4 kan inntreffe»:
STRENGT FORTROLIG nyttes dersom det vil kunne forårsake betydelig skade for offentlige interesser, en bedrift, institusjon eller enkeltperson at dokumentets innhold blir kjent for uvedkommende.
FORTROLIG nyttes dersom det vil kunne skade offentlige interesser, en bedrift, institusjon eller enkeltperson at dokumentets innhold blir kjent for uvedkommende.
§6: «Når et dokument graderes, skal det angis hvilken bestemmelse i offentleglova som gir hjemmel for å unnta dokumentet fra offentlighet. Videre skal angis at graderingen er foretatt i henhold til Beskyttelsesinstruksen».

Alle som skal behandle eller ha tilgang til beskyttet informasjon plikter å sette seg inn i beskyttelsesinstruksen.

Beskyttelsesinstruksen
https://lovdata.no/dokument/INS/forskrift/1972-03-17-3352

6.4.4 Offentlighetsloven

«Lov om rett til innsyn i dokument i offentleg verksemd» skal sikre at alle kan få innsyn i saksdokumenter i offentlig forvaltning. I utgangspunktet er alle saksdokumenter i forvaltningen offentlige. Loven inneholder en del unntaksregler, og når et dokument ikke skal gjøres tilgjengelig for alle, merkes det med «Unntatt offentlighet», og en henvisning til den relevante paragrafen.

Offentlighetsloven
https://lovdata.no/dokument/NL/lov/2006-05-19-16
Forskrift til offentlighetsloven
https://lovdata.no/dokument/SF/forskrift/2008-10-17-1119?q=offentlighetsloven

6.4.5 Lov om bokføring (bokføringsloven)

I henhold til bokføringsloven § 13 annet ledd, skal som hovedregel regnskapsmaterialet oppbevares i Norge.

6.4.5.1 Bokføringsloven

https://lovdata.no/dokument/NL/lov/2004-11-19-73?q=bokf%C3%B8ringsloven

6.4.6 EUs personvernforordning (GDPR)

Personvernforordningens formål er å sørge for en god beskyttelse av personopplysninger, samtidig som personopplysninger skal kunne utveksles fritt innenfor EU/EØS-land.
I artikkel 45 til 47 stilles det egne krav for overføring av personopplysninger til stater utenfor EU/EØS-land

Personopplysninger skal behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak (artikkel 5 bokstav f).

Hovedreglene om informasjonssikkerhet er beskrevet i forordningens artikkel 32. Det stilles krav til at informasjonssikkerheten skal være tilfredsstillende med hensyn til personopplysningenes konfidensialitet, integritet, tilgjengelighet. Tilfredsstillende informasjonssikkerhet skal oppnås ved at egnede tekniske og organisatoriske sikringstiltak iverksettes på bakgrunn av risikovurderinger.

UNINETT - veileder personvernsforordningen
https://www.uninett.no/personvernforordningen-gdpr

Datatilsynets samleside ifm. personvernsforordningen
https://www.datatilsynet.no/regelverk-og-skjema/nye-personvernregler/

6.4.7 Arkivloven

Bestemmelsene i arkivloven skal sikre en helhetlig samfunnsdokumentasjon. Loven har som formål å sikre arkiv som har betydelig kulturell eller forskningsmessig verdi, eller som inneholder rettslig eller viktig forvaltningsmessig dokumentasjon, slik at disse kan bli tatt vare på og gjort tilgjengelige for ettertiden (§ 1)

Arkivloven
https://lovdata.no/dokument/NL/lov/1992-12-04-126

Arkivforskriften
https://lovdata.no/dokument/SF/forskrift/2017-12-15-2105

6.5 Verktøykassen (barrierer)

Azure og Office 365 tilbyr et bredt sett med verktøy som en kan plukke av for å oppnå ønsket beskyttelse av informasjon. Noen av disse verktøyene krever ekstra lisens, mens andre er inkludert.

Verktøykassen består av, men er ikke begrenset til (fortløpende utvikling), følgende verktøy:

Barriere	Forklaring	Kommentar	Type
Brukernavn og passord	Styres av AD lokalt/FEIDE	Kompleksitet og frekvens på bytte av passord bidrar til økt beskyttelse	Barriere
Multifaktor autentisering	Kan aktiveres i FEIDE og/eller i AzureAD		Barriere
Office365 grupper	I "privat" gruppe vil kun medlemmer ha tilgang. I "public" gruppe vil alle i tenant ha tilgang.		Barriere
SharePoint SiteCollection	Forvaltet informasjonsarkitektur og tilgangskontroll		Barriere
IRM / RMS	Information Rights Management		Barriere
Azure Information Protection	Klassifisering og kryptering av innhold		Barriere
Conditional access policy	Kan kreve multifaktor på enkelte innholdselementer som en «SharePoint SiteColl»	Krever ekstra lisensiering	Barriere
Azure RMS portal	For sporing av beskytta dokumenter	1)	Verktøy
S/MIME	Secure Email certificate	2)	
Office 365 Secure Score	Office 365 Secure Score is a security analytics tool	3)	Verktøy
Office 365 Security and Compliance		4)	Verktøy
Lockbox		5)	
Hold your own key - HYOK	Toxic data	6)	
Office 365 - Customer Key		7)	

1. https://portal.azurerms.com/
2. https://www.youtube.com/watch?v=KmfxCd5ubll
3. https://securescore.office.com/
4. https://technet.microsoft.com/en-us/library/dn532171.aspx
5. https://blogs.office.com/en-us/2015/04/21/announcing-customer-lockbox-for-office-365/
6. https://blogs.technet.microsoft.com/solutions_advisory_board/2017/05/09/yes-you-can-put-toxic-data-in-office-365/
7. https://techcommunity.microsoft.com/t5/Security-Privacy-and-Compliance/GA-of-Customer-Key-in-Office-365-at-Ignite/ba-p/115134

Se også: https://products.office.com/nb-no/business/office-365-trust-center-security

6.6 Lisensiering

Crayon er gjennom rammeavtale (https://www.uninett.no/microsoftlisenser) med UNINETT leverandør av Microsoft-lisenser i UH-sektoren.

Det finnes forskjellige type Office 365 lisensiering A1, A3 og A5. Det er også mulig å kjøpe på "Enterprise Mobility + Security (EMS)" lisenser E3 og E5, som tillegg. Innenfor disse lisens-typene er det forskjellig funksjonalitetsgrad som støtter opp under behov for lagring av fortrolig informasjon i Office 365.

- A3 inkluderer EMS E3 funksjonalitet
- A5 inkluderer EMS E5 funksjonalitet

Prosjektgruppen har ikke brukt mye tid på å sette seg inn i detaljene rundt hvilken lisens som gir hvilke muligheter, men har konkludert med at en A3 lisens gir funksjonaliteten som er benyttet innenfor prosjektgruppens Proof of Concept. Dette inkluderer IRM beskyttelse av dokumentbibliotek og basis bruk av AIP.

For å benytte "Conditional access" (https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-azure-portal) kreves Azure AD Premium / Enterprise Mobility + Security lisens.

Lockbox og Office 365 customer key er funksjonalitet som krever A5 lisens.

Andre relevante linker:

- https://technet.microsoft.com/en-us/library/mt844095.aspx
- https://www.microsoft.com/en-us/cloud-platform/enterprise-mobility-security-pricing
- https://azure.microsoft.com/nb-no/pricing/details/active-directory/
- https://www.microsoft.com/en-us/cloud-platform/azure-active-directory-features

Se http://startpakke.uhsky.no/docs/saas/office365/lisensiering/ for mer informasjon.

6.7 Klassifisering – eksempler fra NTNU

Prosjektgruppen har benyttet UNINETT UFS136 som grunnlag i sitt arbeid. Som ett påbygg til det som er skrevet i denne UFS'en har prosjektgruppen diskutert og kommet frem til at det er behov for en klassifisering "Privat". Med større bruk av BYOD vil ansatte benytte seg av egne/hjemme PC'er som de lagrer privat data på og derfor vil det være behov for å skille jobbrelatert informasjon fra private gjøremål.

«Privat» er en klassifisering som går på eierskap til data, mens «Åpen», «Internt», «Fortrolig» og «Strengt Fortrolig» er klassifiseringer som går på behov for beskyttelse. I lys av dette er det anbefalt at «Privat» bør behandles som «Internt» klassifisert data – når det gjelder hvordan arbeidsgiver skal forholde seg til denne type data.

Notis: Innad i prosjektgruppen er det ulik vurdering av om en må ha hjemmel i lov for å benytte begrepene "Fortrolig" og "Strengt Fortrolig". Det er i UFS136 ingen føring om at en må ha lovhjemmel for å benytte disse. Det er opp til hver enkelt institusjon å stå inne for sin bruk av klassifiseringen.

Eksempel på bruk av klassifiseringene:

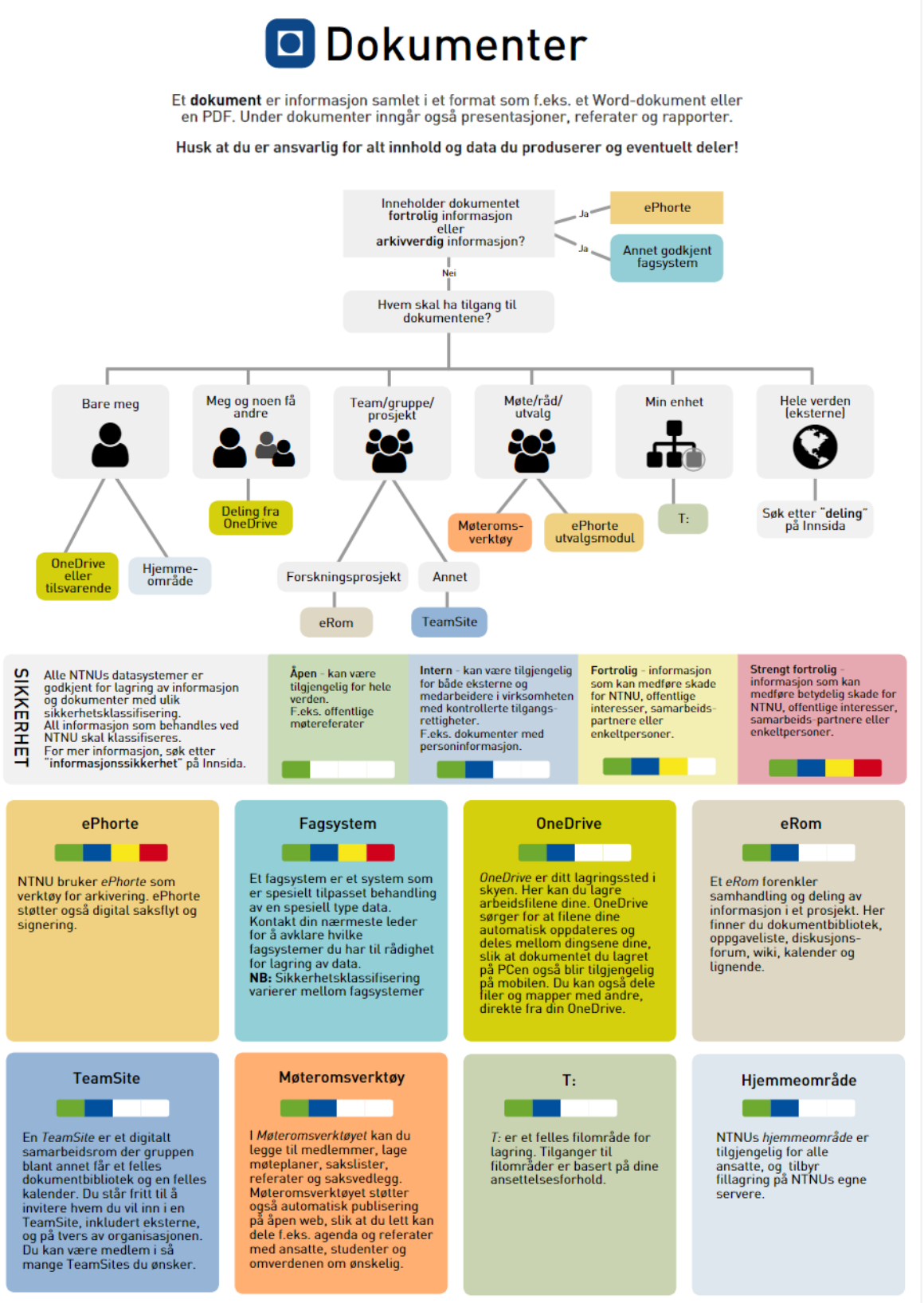
Klassifisering	Konfidensialitet (K)	Integritet (I)	Tilgjengelighet (T)
Nivå 1	**Åpen** informasjon som er tilgjengelig for alle uten særskilte tilgangsrettigheter. Informasjon som ikke kan skade noe eller noen, og alle kan få se. Eksempler på informasjon: Åpen kilde informasjon, offentlige websider, kursoversikter og innhold.	Feil påvirker ikke beslutningsprosesser Arbeidsdokumenter, hvor feil i informasjonen ikke får negativ konsekvens i beslutningsprosesser hos den/de som benytter informasjonen.	Nedsatt ytelse eller utilgjengelighet til informasjon eller tjeneste har liten eller ingen betydning for NTNUs totale produksjon eller omdømme. Begrenset tilgang kan oppleves som kritisk for enkeltperson(er). Feilretting skjer kun innenfor normal arbeidstid.
Nivå 2	**Intern** benyttes om informasjon som er begrenset til å være tilgjengelig for medarbeidere for å gjennomføre pålagte oppgaver. Informasjonen kan være tilgjengelig for eksterne med kontrollerte tilgangsrettigheter. Informasjon på avveie kan gi moderate økonomiske skader og/eller svekket omdømme for NTNU, enkeltindivider eller samarbeidspartnere hvis den kommer uautoriserte i hende.	Den som benytter informasjonen forventer at den er autentisk og gyldig. Feil i informasjonen kan gi moderate økonomiske skader og/eller svekket omdømme for NTNU, enkeltindivider eller samarbeidspartnere.	Nedsatt ytelse eller utilgjengelighet kan føre til noe etterslep i produksjon og redusert servicenivå for store deler av NTNU. IKT-infrastruktur og data kan være utilgjengelig i 2 virkedager uten at det medfører vesentlig fare for økonomisk- eller omdømmetap for NTNU. Feilretting skjer kun innenfor normal arbeidstid.

Nivå 3	**Fortrolig** benyttes dersom det vil kunne skade offentlige interesser, NTNU, enkeltindivider eller samarbeidspartnere at dokumentets innhold blir kjent for uvedkommende. Informasjon som er omfattet av lovbestemt og avtalemessig taushetsplikt. Informasjon skal kun være tilgjengelig for medarbeidere med kontrollerte rettigheter og som har behov for denne informasjonen for å utføre en pålagt oppgave. I spesielle tilfeller kan fortrolig informasjon også gjøres tilgjengelig for eksterne under samme kontrollerte tilgangsrettigheter. Informasjon på avveie som kan medføre alvorlig skade for NTNUs formål, samarbeidspartnere, enkeltpersoner og/eller samfunnet om den kommer uautoriserte i hende. Brudd på konfidensialiteten kan medføre stort økonomisk tap eller alvorlig tap av omdømme.	Den som benytter informasjonen er avhengig av at den er autentisk og gyldig. Utilsiktet eller tilsiktet feilinformasjon vil kunne føre til feilvurderinger eller beslutninger slik at det kan medføre betydelig økonomisk tap, omdømmetap eller annen skade for NTNU, enkeltindivider eller samarbeidspartnere. Dette kan være, men ikke begrenset til; Grunndata, forskningsdata og publikasjoner hvor autentisitet er svært viktig.	Nedsatt ytelse eller utilgjengelighet kan føre til store etterslep eller stans i vesentlige tjenesteleveranser. Systemet eller tjenesten kan maksimalt være utilgjengelig i 4 timer uten at det medfører vesentlig fare for økonomisk- eller omdømmetap for NTNU. Feilretting starter umiddelbart og fortsetter inntil feilen er løst.
Nivå 4	**STRENGT FORTROLIG** benyttes dersom det vil kunne forårsake betydelig skade for offentlige interesser, NTNU, enkeltindivider eller samarbeidspartnere at informasjonen blir kjent for uvedkommende. Informasjon skal kun være tilgjengelig for medarbeidere med strengt kontrollerte rettigheter og som har behov for denne informasjonen for å utføre en pålagt oppgave. I spesielle tilfeller kan	Det er av kritisk betydning at det avleveres autentisk og gyldig informasjon. Utilsiktet eller tilsiktet feilinformasjon vil kunne føre til feilvurderinger eller beslutninger med fatale konsekvenser. Feil i informasjonen kan medføre tap av liv, for eksempel ved feilbehandling av pasienter, eller feilkonstruksjoner i bygg.	Benyttes der nedsatt ytelse eller utilgjengelig kan være katastrofalt. Dvs. selv korte avbrudd vil føre til kritiske situasjoner, f. eks ved gjennomføring av eksamen, utbetaling av lønn, mv. IKT-infrastrukturen har høyeste prioritet, feilretting starter umiddelbart og fortsetter inntil feilen er løst.

	strengt fortrolig informasjon også gjøres tilgjengelig for eksterne under samme strengt kontrollerte tilgangsrettigheter. Brudd kan medføre katastrofal skade på NTNUs interesser, samarbeidspartnere, enkeltpersoner og samfunnet om den kommer uautoriserte i hende. Brudd kan medføre tap av liv. F. eks ved at informasjon om personer med beskyttelsesbehov kommer på avveie. Brudd kan medføre stort økonomisk tap og/eller omdømmetap som får langvarig negativ konsekvens for oppnåelse av NTNUs formål. F. eks. ved at betydelig forskningsmateriale går tapt, eller forskning med militære interesser kommer på avveie. Brudd som kan medføre manglende respekt for den enkeltes liv, integritet og menneskeverd.	Brudd kan medføre korrupte data i sentrale systemer som fører til omfattende følgefeil og påfølgende stort tap av produsert materiale ved NTNU.	

Det er god praksis å ikke overklassifisere. Klassifiseringen "Strengt Fortrolig" bør kun vurderes i særlige/spesielle tilfeller, der det gjør betydelig skade om fremmede skaffer seg uberettiget tilgang til data.

6.7.1 NTNU – Utkast til informasjon omkring god praksis for lagring og klassifisering



Figur 4 - Illustrasjon som viser hvilke systemer som kan benyttes for de ulike klassifiseringene

6.8 Roadmap / hva kommer / dagens begrensninger

Microsoft har ett stort fokus på å forbedre og videreutvikle funksjonalitet som omhandler lagring og deling av fortrolig informasjon, med Azure Information Protection (AIP) som fokus. I dette arbeidet legger Microsoft stor vekt på tilbakemelding fra brukerne gjennom bruk av UserVoice:

https://msip.uservoice.com/forums/600097-azure-information-protection/filters/top

Per februar/mars 2018 er blant annet følgende funksjonalitet identifiserte element i "Roadmap":

- SharePoint Online Support for AIP – mulighet til å automatisk sette AIP label på dokumentbibliotek i SharePoint Online.
- Det jobbes med bedre support for MacOS / Office for Mac. Preview på AIP for Office på Mac er på slutten av prosjektgruppens POC utgitt.
- Bedre suppport for AIP håndtering av PDF-filer.

Fra Ignite 2017:

- https://www.youtube.com/watch?v=9mQKO1lVzOI&t=5s

6.9 Backup/restore, logging, DLP

6.9.1 Backup/restore

Standardinnstillinger i Office 365 er følgende:

- OneDrive for Business filer kan gjenopprettes 30 dager etter at en bruker er merket for sletting.
- SharePoint/OneDrive filer slettes permanent etter 93 dager.

Default restore muligheter i SharePoint online:
http://icansharepoint.com/restoration-options-sharepoint-online

Retention policies:
https://support.office.com/en-us/article/overview-of-retention-policies-5e377752-700d-4870-9b6d-12bfc12d2423

6.9.2 Logging

Det er god praksis å skru på audit logging på epostbokser i Exchange Online:
https://support.office.com/en-us/article/enable-mailbox-auditing-in-office-365-aaca8987-5b62-458b-9882-c28476a66918

Overview of Audit Options for SharePoint Online Activities:
https://blogs.technet.microsoft.com/sposupport/2017/10/25/overview-of-auditing-options-for-sharepoint-online-activities/

6.9.3 DLP - Data loss prevention

DLP lar deg identifisere sensitive data og opprette policyer som vil hindre brukerne i ved et uhell eller med hensikt deling av dataene. DLP fungerer i Office 365, inkludert Exchange Online, SharePoint Online og OneDrive slik at brukerne kan holde kompatibel uten å avbryte arbeidsmåten deres

https://support.office.com/nb-no/article/overview-of-data-loss-prevention-policies-1966b2a7-d1e2-4d92-ab61-42efbb137f5e?ui=nb-NO&rs=nb-NO&ad=NO

6.10 Kompatible filtyper

File formats that work with IRM
https://support.office.com/en-us/article/file-formats-that-work-with-irm-d5d82a8e-e257-4518-a282-6ed0ae13eb63

File types supported by the Azure Information Protection client
https://docs.microsoft.com/en-us/information-protection/rms-client/client-admin-guide-file-types

6.11 Versjonshistorikk

- V0.5 - 01.03.2018 – Utkast til endelig rapport (høringsrunde)
- V0.6 - 13.03.2018 - Små justeringer etter intern høringsrunde.
- V1.0 - 22.03.2018 - Tatt inn kommentarer fra høringsrunde.
- V1.0.1 – 16.04.2018 – Oppdatert figure i Kap. 1.2.1