

Dokumentklasser og lagringssteder

Klasse	Hvem har tilgang / type data	Merknader
 Åpen	Informasjon kan eller skal være tilgjengelig for alle uten særskilte tilgangsrettigheter. Eksempler på slik informasjon er en web-side som legges åpent ut på internett.	Skal ikke kreve innlogging eller annen form for identifikasjon, autentisering og autorisering. Integritet er fortsatt like viktig.
 Intern	Data som er beregnet kun for UIS-ansatte, studenter ved UIS eller navngitte enkeltpersoner eller grupper ved institusjoner UIS samarbeider med. Eksempler på slik informasjon er enkelte arbeidsdokumenter, informasjon som er unntatt offentlighet, enkelte personopplysninger, karakterer, studentarbeider, eksamensbesvarelser og upubliserte forskningsdata og -arbeider.	Tilgang skjer etter innlogging med brukernavn og passord.
 Fortrolig	Dette er informasjon som universitetet er pålagt å begrense tilgangen til i lov, forskrift, avtaler, reglementer og annet regelverk. «Fortrolig» benyttes hvis det vil forårsake skade for offentlige interesser, universitetet, enkeltperson eller samarbeidspartner om informasjonen blir kjent for uvedkommende. Eksempler på slik informasjon er enkelte strategidokumenter, særskilte personopplysninger, helseopplysninger, informasjon om sikring av bygninger og IT-systemer, eksamensoppgaver før de er gitt, enkelte typer forskningsdata og -arbeider.	Tilgang skjer etter innlogging med brukernavn og passord. To-faktor autentisering* ved bruk av skyløsning. Bærbare enheter: PC, Mac, USB-pinner og -disker må krypteres* Dokumenter som lagres i Office365 (f.eks i Teams) krever ekstra beskyttelse og må derfor merkes med etiketten «Fortrolig» **
 Strengt fortrolig	Strengt fortrolig benyttes dersom det vil kunne forårsake betydelig skade for offentlige interesser, institusjonen, enkeltperson eller samarbeidspartner at informasjonen blir kjent for uvedkommende. Informasjonen skal ha de strengeste tilgangsrettigheter. Eksempler på slik informasjon er store mengder sensitive personopplysninger, store mengder helseopplysninger eller forskningsdata og datasett av stor økonomisk verdi.	Plassering av data og informasjon i denne kategorien gjøres i samarbeid med UIS jurister og IT-sikkerhetsteam.

*) Ta kontakt med UIS-IT mht. kryptering og to-faktor autentisering

**) Etiketter (labels) vil innføres i løpet av 2020

Hvor kan jeg lagre	Hva kan jeg lagre	Klasse	Merknader
 OneDrive for Business	Dine personlige jobbfiler og filer som skal deles med ganske få personer i kortere perioder (1-2 personer). Overtar for F:/ -området	 	Du har 1Tb lagringsplass tilgjengelig. Synkroniseres til din PC.  Lagre fortrolig? Ta kontakt med UiS-IT
 Microsoft Teams	Samarbeid og deling for prosjekter og aktiviteter. Overtar for G:/ -området	 	Husk at Teams alltid bør ha to eiere.  Lagre fortrolig? Ta kontakt med UiS-IT
 Microsoft Outlook	Epost og vedlegg til epost.	 	Synkroniseres til din PC
 Office 365 grupper  Microsoft SharePoint	Samarbeid og deling for prosjekter og aktiviteter.	 	Husk at O365 grupper og SharePoint alltid bør ha to eiere.  Lagre fortrolig? Ta kontakt med UiS-IT
 Public 360	Alle arkivverdige filer.	  	Kontakt UiS-IT for evt. mer informasjon om arkivverdighet.
 TSD	Forskningsdata inneholdende sensitive data, også personsensitive.	 	Bestilles hos UiS IT. Tjenesten leveres av UiO.
 USB-enhet kryptert	Filer som er for en, eller et begrenset utvalg personer.	  	Minnepinne med innebygd kryptering kan bestilles i portalen (for ansatte).
 USB-enhet, åpen	Filer som alle kan se.		Ikke benytt enheter du ikke har kontroll over.
 Intranett	Åpen og intern informasjon.	 	Kun for ansatte. Krever pålogging for tilgang.
 Internett	Åpen informasjon.		For alle - www.uis.no - student.uis.no