Oppskrift på å sende sensitive filer via epost

Utarbeidet av Asle Orseth. Versjon 2. 16.01.2020

Denne guiden omhandler hvordan man kan sende sensitive filer via epost for ansatte på Seksjon for Innkjøp. For vår del handler det typisk om tilbudsfiler og kontraktsinfo med priser o.l. som inneholder taushetsbelagt informasjon. Guiden er derfor skrevet med anskaffelsesrådgiverne i bakhodet, men det vil sikkert være overførbart også i andre sammenhenger.

Når kan man sende sensitiv info på epost?

Ihht UiOs egen klassifisering så vil nok de fleste tilbudsfiler regnes som enten røde eller gule data. Disse må beskyttes mot uønsket innsyn. Epost er i utgangspunktet ingen sikker måte å sende informasjon på.

På tross av det oppgir UiOs lagringsguide at sensitive data kan sendes pr epost, men kun dersom følgende kriterier er oppfylt:

1. Mottakeren må være ansatt i UiO, og epostadresse for både avsender og mottaker må være en UiO-adresse
2. Man gjør nødvendige tiltak for å sikre at sensitiv informasjon ikke kommer på avveie. Dette innebærer at sensitiv info ikke skal lastes ned til hjemmeområdet eller lagres på andre steder som ikke er sikret.

Om mottakeren er ekstern må eposten krypteres. Dette er teknisk vanskeligere, og det vil jeg ikke gå inn på i denne guiden. Jeg vil tro det uansett er begrenset hvor ofte man har behov for å sende slike filer til eksterne. Det er vel gjerne ifm kommunikasjon med eksisterende leverandør, og da kan man dele filer via Visma Tendsign.

Hvordan?

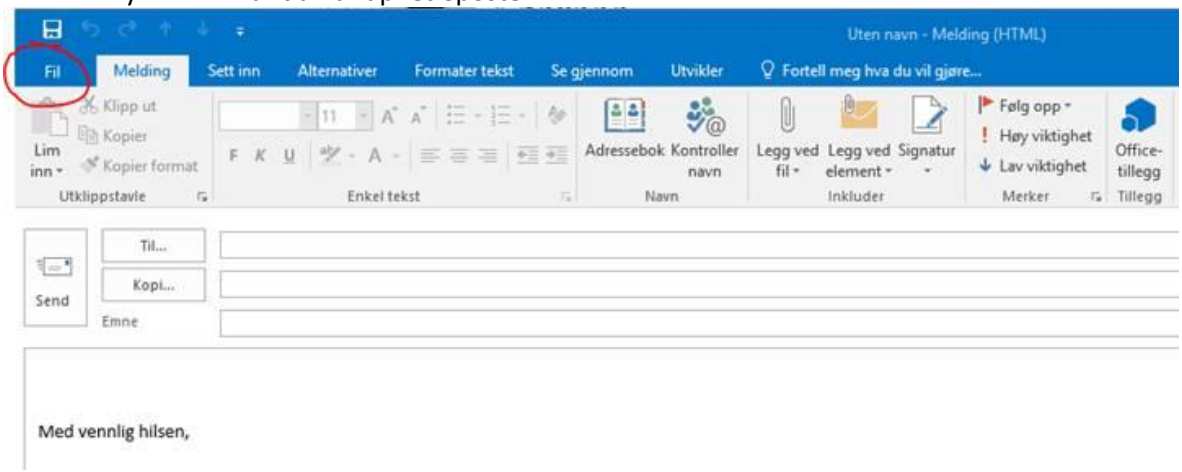
Dersom forutsetningen om at epostmottakeren er en intern adresse er oppfylt, må man likevel sikre at sensitiv informasjon ikke kommer på avveie.

Det finnes 2 alternative fremgangsmåter for dette. Det ene er å sette en enkel sikkerhetssperre på selve eposten. Det andre er å kryptere de enkelte vedleggene.

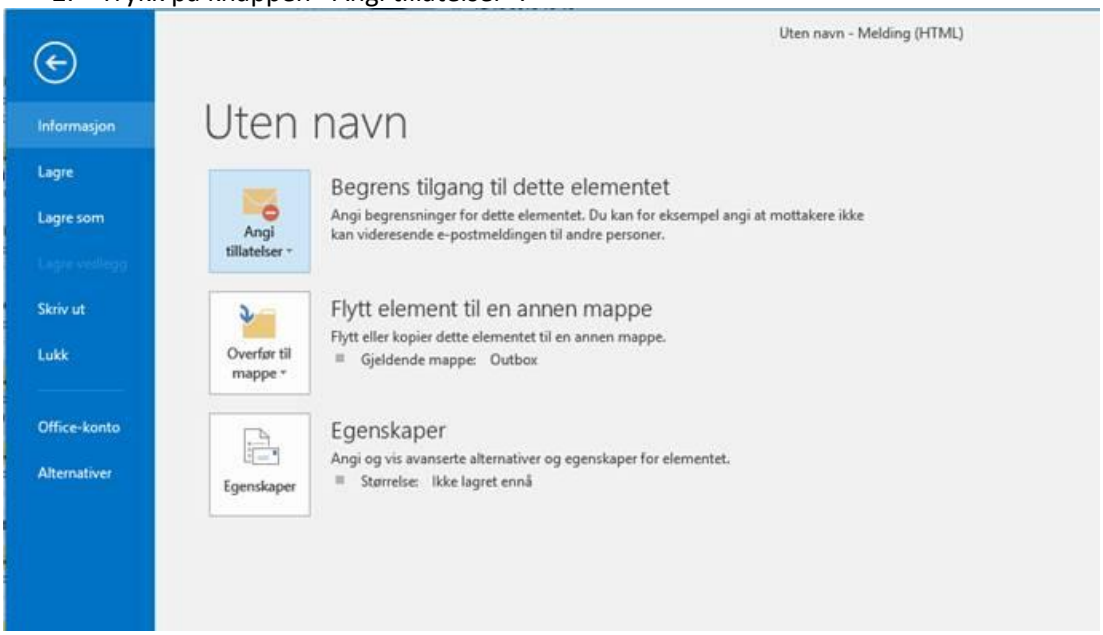
ALTERNATIV 1: SIKKERHETSSPERRE PÅ EPOSTEN:

Det finnes et verktøy i Outlook som er til hjelp:

1. Trykk «Fil» når du har åpnet eposten



2. Trykk på knappen «Angi tillatelser»:



3. Du skal da få en nedtrekksmeny med 4 valg. Velg «Universitetet i Oslo – confidential view only».

   Dette medfører at mottakeren kun kan se, men ikke videresende eller skrive ut eposten. Merk at mottaker heller ikke kan svare deg, og må henvises til å sende en separat epost dersom det er nødvendig. Om man i stedet velger «Universitetet i Oslo – confidential», kan mottakeren svare og videresende, men da mister man noe av sikkerheten i funksjonaliteten. Dette er derfor ikke anbefalt.

4. Mottakeren får opp info om at meldingen er sikret:

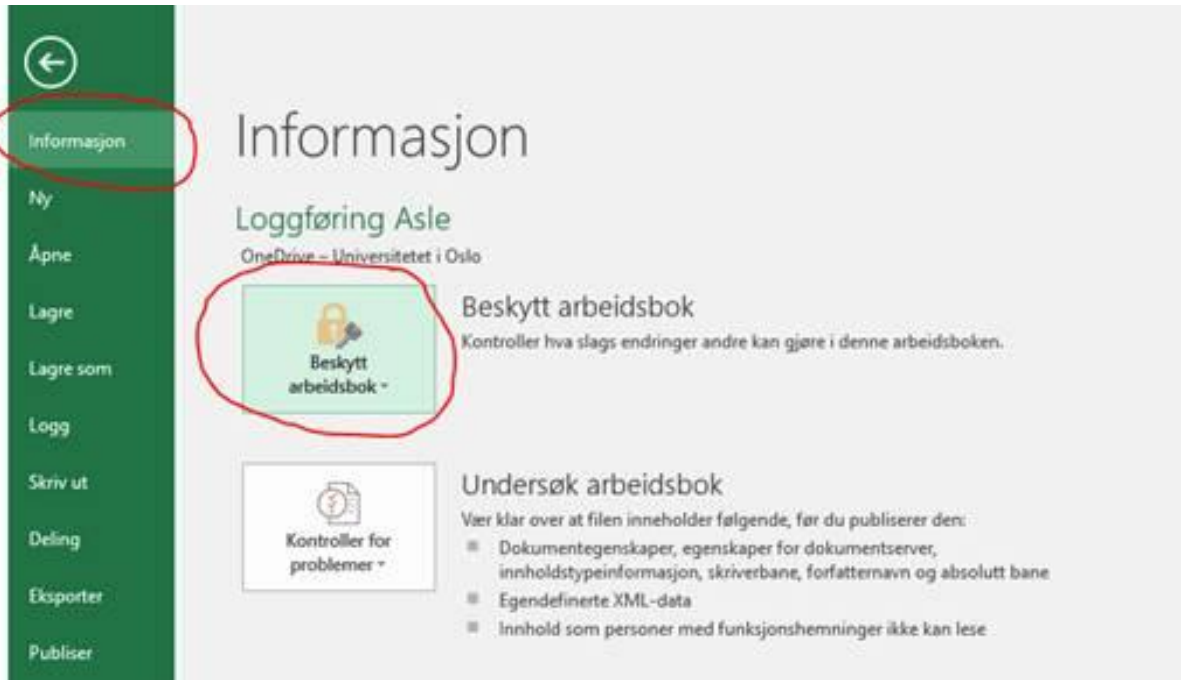
   Mottakeren må sitte ved en PC som er koblet mot UiO sitt nettverk og som har Outlook installert for å se innholdet i eposten. Dersom dette er første gang mottaker mottar en sikker epost vil Outlook automatisk starte en nedlasting for å kontrollere rettighetene til mottaker. Dette går relativt raskt, men det er avgjørende at mottaker ikke avbryter denne.

Om man i tillegg til denne fremgangsmåten opplyser mottakeren om at eposten inneholder taushetsbelagt informasjon, som man ikke kan dele videre eller lagres på hjemmeområdet, så bør man etter mitt syn ha oppfylt de interne kravene til sikring.

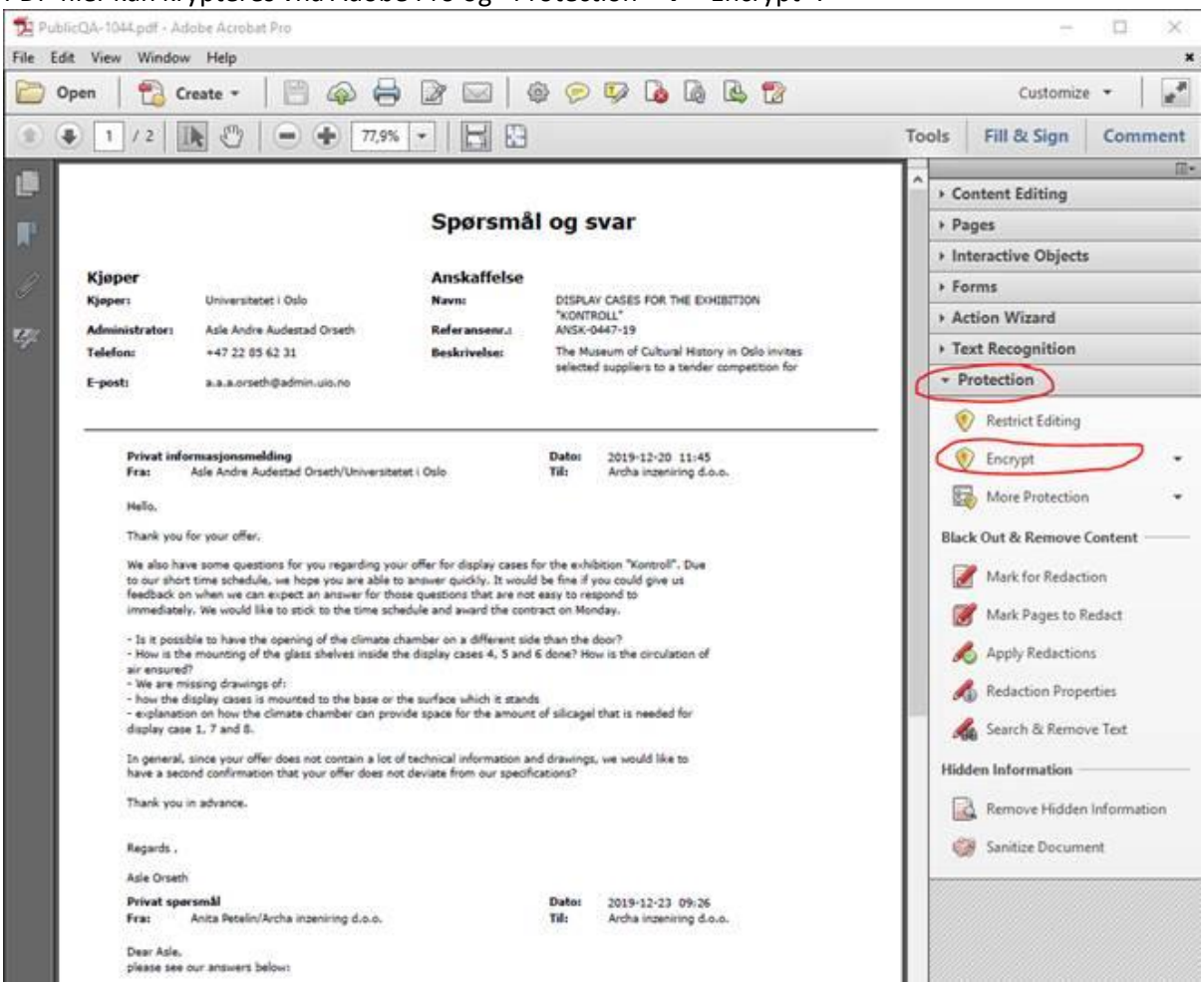
ALTERNATIV 2: KRYPTERING AV VEDLEGG:

Denne fremgangsmåten innebærer at man sender selve eposten på vanlig måte, men at man sikrer hver enkelt av de vedlagte filene med et passord. Dette forutsetter at det ikke er sensitiv info i selve epostteksten. Husk å sende passordet til mottaker på en annen måte enn via epost (for eksempel som sms).

De fleste Office-filer (word, excel, powerpoint m.fl.) kan sikres/krypteres ved å trykke på «Fil» → «Informasjon» → «Beskytt arbeidsbok/dokument/presentasjon». Dette gjør du inne i selve Office-dokumentet:



PDF-filer kan krypteres vha Adobe Pro og «Protection» → «Encrypt»:



Alternativer?

Det finnes andre måter å dele informasjon med interne mottakere på, som i utgangspunktet er sikrere:

1. Gi tilgang til brukere i Visma Tendsign
2. Gi tilgang til brukere i ePhorte
3. Dele info direkte i fysiske møter

Det finnes sikkert flere metoder som jeg ikke kommer på også. Men i mangel på tid, teknisk kompetanse hos mottaker eller andre årsaker kan man enkelte ganger likevel ha behov for en enklere måte å dele filer på. Da kan de to fremgangsmåtene som jeg har beskrevet være et alternativ.

Merk at å dele sensitive filer i Onedrive/Skype for business/Dropbox/Google Drive etc ikke anses som sikkert nok.