SYKEHUSET I VESTFOLD

Informasjonssikkerhet - kryptering av Office 2016 dokumenter

Gjelder for:	[]
Dokumenttype:	Prosedyre
Sist endret:	30.08.2018

1. HENSIKT

Denne prosedyren viser deg hvordan du kan beskytte dine dokumenter i Microsoft Office 2016 gjennom bruk av passord og kryptering, for bruk hvis man skal oversende sensitiv informasjon pr. e-post. HSØ har ingen e-post løsning for kryptert e-post. Fremgangsmåten er lik for de fleste programmet i Microsoft Office-pakken (F.eks Excel, Word og PowerPoint).

2. ANSVAR

Vær bevisst på informasjonens livssyklus. Det betyr å ha en aktiv formening om hvordan informasjon skapes, oppbevares/brukes og til sist slettes. Det kan være lurt at avdelingen har retningslinjer for dette (gjerne en «arkivansvarlig») som gjør rutinene kjent og forstått i avdelingen.

3. FREMGANGSMÅTE

Husk før du krypterer

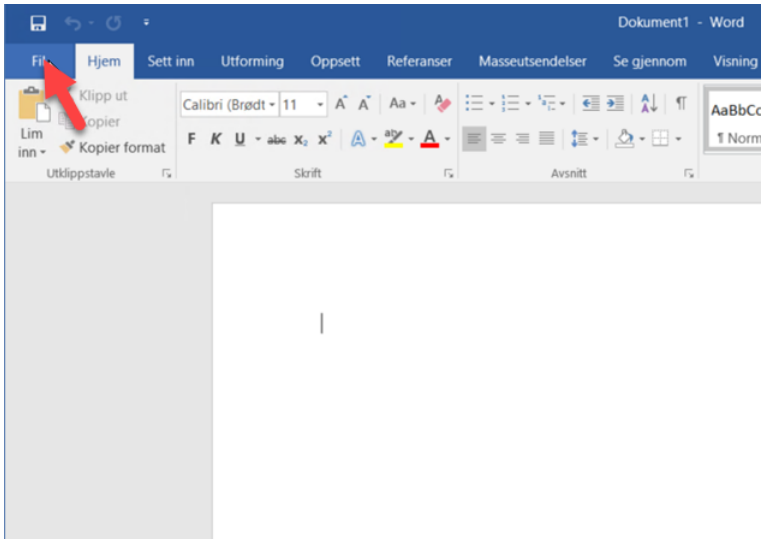
Når dokumentet er kryptert kan det bare leses og endres av noen om kjenner passordet. Vær derfor varsom slik at du ikke mister informasjon ved tapt passord.
Det oppnås ikke god beskyttelse om dokument og passord lagres på samme sted.
Dersom du skal distribuere dokumentet over e-post er det best å dele passordet over en annen kanal, f.eks via SMS eller over telefon. Merk at direktemelding (chat) er ikke egnet for utveksling av passord, siden passordet kan bli lagret i meldingsloggen.

Hvor sikker er krypteringen?

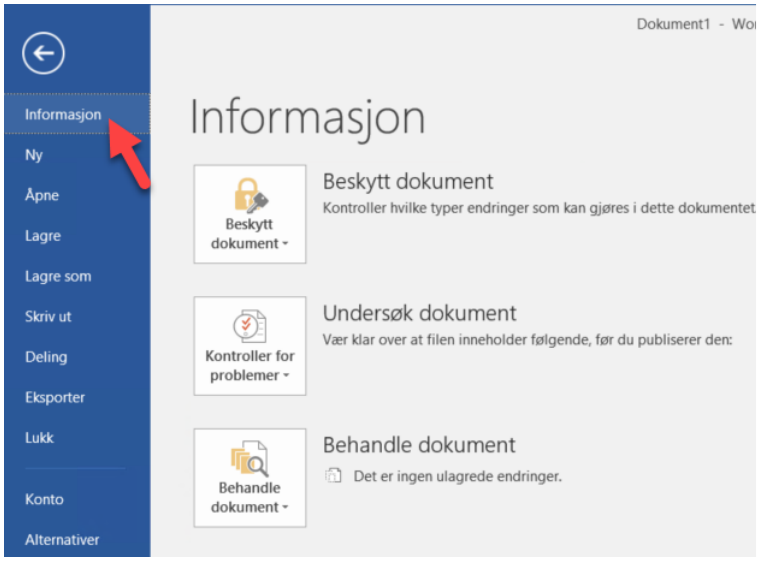
Krypteringen i Microsoft Office 2016 er regnet som sikker (AES med 256-bit-nøkkel) og tar svært lang tid å knekke med dagens maskinressurser om passordet er godt nok.

Se prosedyren Fellesregional autentiseringspolicy for tips til hvordan du kan lage gode og sikre passord.

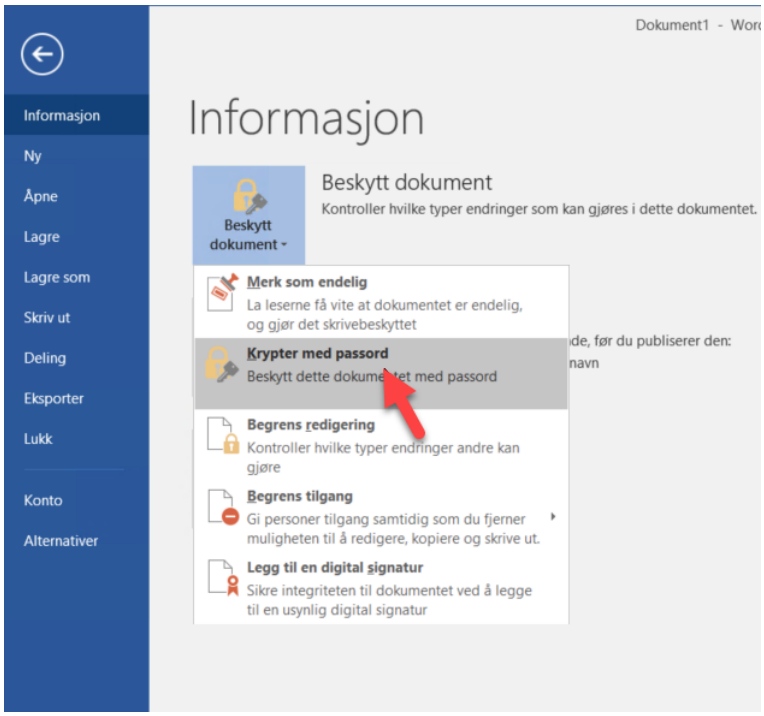
1. Åpne dokumentet du vil kryptere. Viktig at det er i .docx, .xlsx eller .pptx format. Trykk deretter på **Fil**



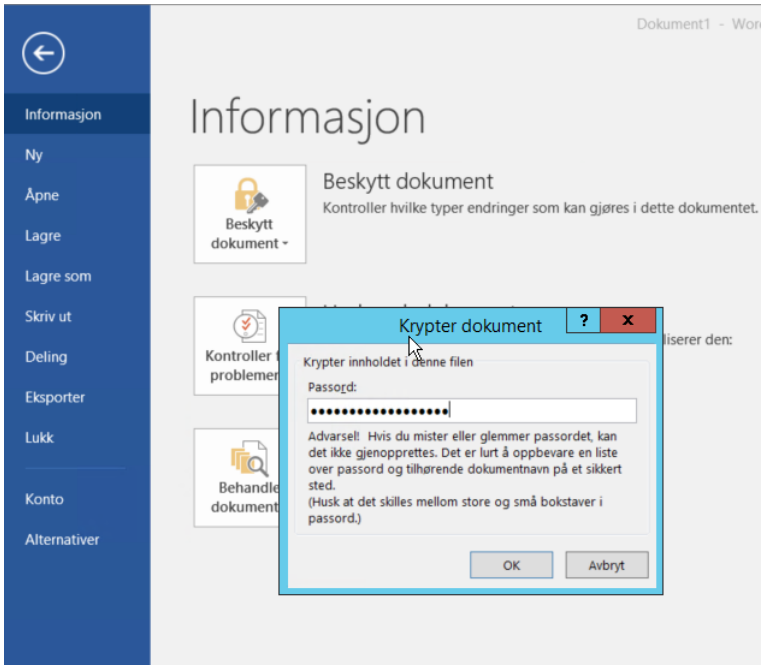
2. I neste vindu, trykk **informasjon** øverst til venstre.



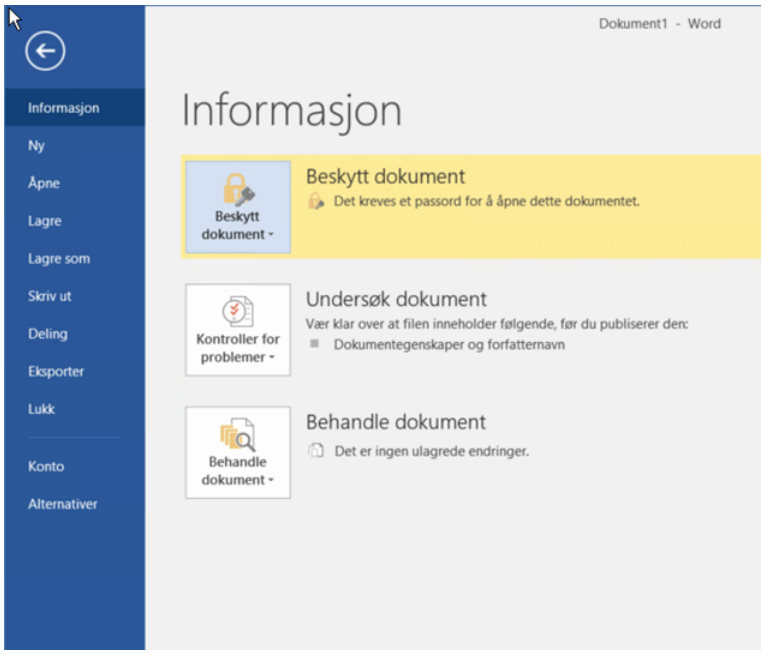
3. Trykk **Beskytt dokument**, og deretter **Krypter med passord**.



4. I dialogboksen som dukker opp skriver du inn ønsket passord. Husk å lage et godt passord.
   Trykk deretter **OK** og du blir bedt om å skrive inn passord på nytt. Trykk **OK**.



5. Du vil nå se at **Beskytt dokument** har endret farge og at teksten gjenspeiler at kryptering er slått på. For å fjerne krypteringen gjentar du de samme stegene, men skriver inn et blankt passord i passordfeltet.



6. Lagre dokumentet og legg dette ved e-post hvis det skal sendes kryptert vedlegg.

4. GENERELT

Tips og råd

- Om SMS benyttes til å overlevere passordet, bør du bevisstgjøre mottager på at meldingen med passordet bør slettes før, eller umiddelbart etter at den krypterte filen er mottatt. Dette fordi SMS gjerne lagres «åpent» på samme mobile enhet som mottakers e-postkasse.
- Man skal ikke ukritisk åpne krypterte filer på maskiner som kan benyttes av uvedkommende. Ved åpning av filer vil det lages en temporær kopi. Normalt slettes denne, men filen har da vært lagret ukryptert på lokal disk og kan gjenskapes.

5. INTERNE REFERANSER

1.1.11.1.4 Sikkerhetsinstruks
1.1.11.1.5 Fellesregional autentiseringspolicy
1.1.11.2.4 Bruk av e-post, SMS, telefaks (digital kommunikasjon)
1.1.12.2.6 Informasjonssikkerhet - Bruk av e-post og fax for kommunikasjon med og om pasienter
1.1.11.2.13 Informasjonssikkerhet - kryptering av minnepinne - Windows 10

6. EKSTERNE REFERANSER

7. VEDLEGG