Makulering

Det er ikke bare digitale verdier vi må beskytte. Vi må også beskytte fysiske dokumenter. Når vi ikke lenger har behov for dokumentene, er det viktig å gjennomføre sikker makulering av dokumenter med sensitivt innhold. Det kan være dokumenter med opplysninger om våre medlemmer, samarbeidspartnere, eller virksomhetsinterne dokumenter.

Sikker makulering følger standarden DIN 66 399. Ifølge standarden skal dokumenter makuleres iht. sikkerhetsnivå P-5.

Kopimaskiner

Alle kopimaskiner (mulitimaskiner, kopi/print) har lokalt minne. Når IT-teknikeren bytter ut slikt utstyr er det viktig å få skrudd ut harddisken. Den inneholder informasjon/personopplysninger og skal avhendes på en sikker måte.

Interne ressurser

Kirkens personvernside

https://www.kirken.no/personvern

Kurs i informasjonssikkerhet og personvern

Det tilbys en rekke kurs i informasjonssikkerhet og personvern i kirkens læringsplattform. Det tilbys også kurs uten innlogging.

Godkjent av Sikkerhetsutvalget 31.05.2023

Avvik og uønskede hendelser

Når vi har en god kultur for å melde avvik og uønskede hendelser kan vi oppnå læring, forebygging og forbedring. Dette gjør oss mer robuste som virksomhet.

Med avvik menes manglende oppfyllelse av et krav. En uønsket hendelse er en hendelse som kan utsette, eller som har utsatt, våre verdier for uønsket påvirkning.

Brudd på interne rutiner, lov eller forskrift er eksempler på avvik. En uønsket hendelse kan for eksempel være at du blir frastjålet en pc eller mobil, eller at du har trykket på en lenke som ikke var trygg.

Ta kontakt

Hvis du har behov for å melde et avvik eller en uønsket hendelse, kan du sende e-post til personvernombudet@kirken.no. Hvis du jobber i et fellesråd så kan du også sette kirkevergen på kopi.

Har du behov for ytterligere informasjon, eller du har spørsmål knyttet til denne folderen, send dette til: infosikkerhet@kirken.no.

Nyttige nettsider

Nettsider med veiledninger og gratis kurs

Norsk senter for informasjonssikring - https://norsis.no/

NettVett.no - https://nettvett.no/

Slettmeg - https://norsis.no/slettmeg/

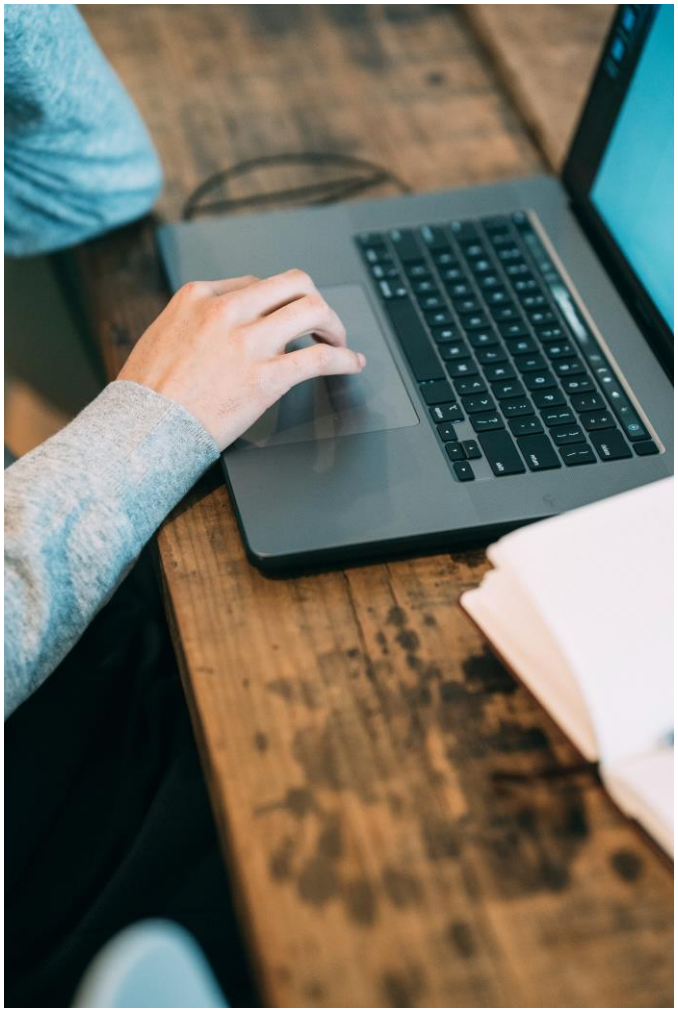
Reiseveileder fra Næringslivets sikkerhetsråd https://www.nsr-org.no/aktuelt/revidert-veileder-i-reisesikkerhet

DEN NORSKE KIRKE

Sikkerhetsutvalget

Digital trygghet

Gode råd som kan gi deg en tryggere digital hverdag



Din digitale trygghet er viktig!

Det digitale trusselbildet utvikles stadig og kirkens ansatte utsettes daglig for digitale angrep. Det er derfor viktig at vi alle bidrar til å sikre trygge digitale løsninger.

Vi bidrar med sikrede digitale tjenester med felles ordning for personvern og informasjonssikkerhet. Likevel er vi avhengig av hver enkelt medarbeiders innsats for å opprettholde kirkens digitale trygghet. Denne folderen skal gi gode og enkle råd som skal bidra til at vi når dette målet sammen.

Sikringstiltakene som du får innsikt i her vil også heve din egen sikkerhet. Dette skaper trygghet både for kirken, våre medlemmer og deg selv.

- Lær deg hvordan du kan avdekke falske e-poster og falske lenker.
- Meld avvik og uønskede hendelser.
- Vær varsom med hva du deler på sosiale medier.
- Etabler flerfaktorautentisering på dine kontoer på sosiale medier.
- Sett passord på pc, mobil og andre mobile enheter.

Husk at du er *sikkerhetssjef* for den informasjonen du behandler.

Med ønske om en trygg digital arbeidsdag!

Jan Rune Fagermoen
Leder for Sikkerhetsutvalget

10 sikkerhetsråd du bør følge

1. Ha alltid kontroll på dine enheter og beskytt dem med et sikkert passord på minst 12 tegn, pin-kode, ansikts-gjenkjenning eller fingeravtrykksmønster.
2. Hvis du må skrive ned passord, oppbevar det i en liten notisbok som du oppbevarer et trygt sted.
3. Aktiver flerfaktorautentisering* på sosiale medier og dine e-postkontoer.
4. Unngå bruk av offentlige og lett tilgjengelige trådløse nettverk. Det er tryggere å bruke mobilnettet (4G/5G).
5. Aldri del passord med andre.
6. Unngå at nettlesere og nettsider husker dine kortopplysninger og passord.
7. Ikke send sensitive personopplysninger med e-post.
8. Vurder nøye om den enkelte app på telefonen trenger tilgang til kontakter, mikrofon, høyttaler, kamera, stedstjenester, mm.
9. Benytt kun din egen mobillader, og bruk alltid en datablokker når du lader mobilen fra ukjente usb-punkter
10. Bruk aldri USB-stasjoner/minnepinner som du ikke vet opprinnelsen til.

*lignende begreper: to-faktor, to-trinnsverifisering og multifaktor

Falske e-poster og lenker

E-post er en nødvendig del av vår digitale hverdag. Dessverre kan e-poster enkelt forfalskes til å fremstå som noe annet enn de er, og det utnyttes daglig av svindlere.

Slik kan du avsløre falsk e-post og e-post med skadelig innhold:

- Se nøye på hvilken adresse e-posten er sendt fra. Velg Svar, som om du skal svare e-posten. Da ser du reell e-postadresse i Til-feltet.
- Ved å holde musepekeren over lenker kan du enkelt se den reelle adressen til nettsiden (ikke klikk før du er sikker).
- Se etter skrivefeil i e-postadresser og lenker. Skrivefeil indikerer falsk avsender og nettadresse.
- Vær varsom hvis e-posten eller vedlegget ikke er ventet, eller om det er for godt til å være sant.
- Oppgi aldri passord eller kortinformasjon via e-post.
- Ikke la noen overtale deg til å omgå dine sikkerhetsrutiner.

Her kan du sjekke vedlegget i e-posten før du åpner det: https://www.virustotal.com. Dra filen fra e-posten og slipp den på nettsiden for virusskanning.