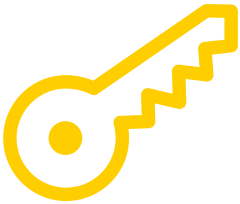
CYBERSIKKERHET FOR
SMÅ VIRKSOMHETER

NorSIS

FYSISK SIKKERHET



Cybersikkerhet starter med fysisk sikring.

Svakheter innen fysisk sikkerhet kan medføre tap/tyveri av bedriftens informasjon, med mulige alvorlige konsekvenser.

En ansatt etterlater ved et uhell en USB-minnepinne, som har hundrevis av personnumre lagret på seg, på et bord i en kaffebar. Når han kommer tilbake en time senere, for å hente minnepinnen, er den borte.

En annen ansatt kaster flere stabler med gamle dokumenter i søpla. Utenfor arbeidsplassen plukker en kriminell opp disse papirene fra søpla.

En tyv stjeler dokumenter og datamaskinen fra kontoret ditt etter å ha kommet seg inn et ulåst vindu.

HVORDAN BESKYTTE UTSTYR OG DOKUMENTER

Her er noen tips for hvordan du kan beskytte informasjon på papir, harddisker, minnepinner, bærbare datamaskiner, salgsenheter, og annet utstyr.

Sikker oppbevaring

Sørg for at fysiske dokumenter eller elektroniske enheter som inneholder sensitiv informasjon er oppbevart i et låst skap eller tilsvarende når de ikke er i bruk.

Begrens fysisk tilgang

Gi bare tilgang til utskrifter eller enheter som inneholder sensitiv informasjon, til de som trenger det.

Send påminnelser

Minn ansatte på å legge papirdokumenter i låsbart skap, logge ut av datamaskinen, og aldri forlate dokumenter eller enheter med bedriftens informasjon uten tilsyn.

nettvett.no/digital-sikkerhetskultur/

Ha oversikt

Hold kontroll på alle enheter som samler inn kundedata. Lagre bare dokumenter og data du trenger, og ha oversikt over hvem som har tilgang til dem.

datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/

CYBERSIKKERHET FOR
SMÅ VIRKSOMHETER

NorSIS

HVORDAN BESKYTTE INFORMASJON PÅ ENHETENE DINE

Tyveri, mistet laptop, stjålet mobiltelefon eller gjenglemt minnepinne – svakheter i fysisk sikkerhet øker sannsynlighet for at dette kan skje. Tap av informasjon er mindre sannsynlig dersom den også beskyttes på de digitale enhetene.

Krev komplekse passord

Krev passord som er lange, komplekse og unike. Om nødvendig, skriv de ned og lagre på et trygt sted. Vurder å bruke et passordhåndteringsprogram.

nettvett.no/passord/

Bruk totrinnsbekreftelse

Krev totrinnsbekreftelse for tilgang til tjenester med sensitiv informasjon. Dette krever et ekstra steg i tillegg til innlogging med et passord – som regel en midlertidig kode på en smarttelefon.

nettvett.no/2-trinns-bekreftelse/

Begrens antall forsøk på innlogging

Begrens antall tillate mislykkede forsøk på innlogging for å låse opp enheter. Dette vil hjelpe til med å beskytte mot inntrengere.

Krypter

Krypter flyttbare enheter, inkludert bærbare datamaskiner og minnepinner som inneholder bedriftens informasjon. Krypter alle sensitive data som sendes utenfor virksomheten.

LÆR OPP DE ANSATTE

Inkluder fysisk sikkerhet i virksomhetens regelmessige opplæringsaktivitetene.

Makuler dokumenter

Makuler alltid dokumenter som inneholder sensitiv informasjon før de kastes.

Følg sikkerhetstiltak på alle områder

Opprettholde bedriftens sikkerhetstiltak, selv når du ikke er på arbeidsplassen.

nettvett.no/ikt-utenfor-kontoret/

Slette data på riktig måte

Bruk programvare til sletting av data før du kvitter deg med gammelt utstyr. Ikke stol på vanlig sletting – dette sletter ikke filene godt nok.

nettvett.no/sikker-sletting/