Skape et trygt IT-miljø

01
INNLOGGING
IT-miljøet beskyttes med Brukernavn og passord. Innloggning bør skje med personlige påloggingsdetaljer som inneholder passord som er vanskelig å gjette. Påloggingsdetaljer skal beskyttes og ikke gjøres tilgjengelige for uvedkommende.

02
LAGRINGSMEDIE
Vær forsiktig med åpning av filer fra lagringsmedie som tilkobles IT-miljøet, f eks USB, CD-DVD, eksterne harddisker og minnekort, da disse kan infisere IT-miljøet med virus eller annen skadelig programvare.

03
E-POST
Vedlegg i e-post fra ukjente avsendere bør aldri åpnes av for å unngå at IT-miljøet infiseres av virus eller annen skadelig programvare.

04
E-POST
Vedlagte filer med ukjent innhold fra kjente e-postavsendere bør åpnes med forsiktighet da virus eller annan skadelig programvare, tilsynelatende fra avsenderen, kan formidles gjennom denne kanal.

05
INTERNETT
Å besøke nettsteder med ulovlig, uetisk eller annen ukjent innhold, samt nedlasting av informasjon fra internett hvor opprinnelsen er ukjent eller fra en usikker kilde, utgjør alltid en sikkerhetsrisiko, med tanke på IT-miljøet.

06
INTERNETT
Unngå å bruke båndbredden og delt Internett-trafikk til private formål. Streaming-tjenester som Spotify, Youtube, Netflix og andre Play-tjenester eller nedlasting av store filer kan påvirke båndbreddenes ytelse.

07
PROGRAMVARE
Mulighet til å installere eller avinstallere programmer bør styres av begrensninger og brukerrettigheter i IT-miljøet. Bare personer med høy IT-kunnskap, som IT-leder, bør ha disse rettighetene.

08
FEILMELDINGER
Ved mistanke om at IT-miljøet ditt er utsatt for risiko eller skade, skal det rapporteres til IT-administratoren så snart som mulig.

Vi vil med disse anbefalte rutiner for IT-sikkerhet gi eksempler på hvordan personer med tilgang til deres IT-miljø bør reagerer i ulike sikkerhetsutfordringer. Anbefalte rutiner fremmer en økt sikkerhet i IT-miljøet som igjen minsker muligheten for angrep.

Disse rutiner er kun anbefalinger og dermed ikke komplette it-rutiner for din bedrift. Alle systemers svakhet er muligheten for manuelle handlinger. Unident tar ikke ansvar for handlinger som skjer på individnivå og deretter ligger på utsiden av Unidents kontroll. Ansvaret for å opprettholde en høy IT-sikkerhet er hos brukerne av IT-miljøet.

UNIDENT®

Adresse: Postboks 1045, 3194 Horten
Telefon: 33 03 57 70
Mail: info@unident.no | **Web:** unident.no