Brug af IT i organisationen

Pixibog

TD-K A/S 2026

Introduktion

Dette dokument udgør en del af et informationssæt om IT-sikkerhed, og det beskriver vores anbefalede forholdsregler for brug af IT i virksomheden.

Regler for brug af IT

Det er hver enkelt medarbejders ansvar at medvirke til, at <kundenavn> til enhver tid og i ethvert forhold lever op til de fastsatte sikkerhedskrav. Alle har pligt til at rapportere mulige svagheder og brud på sikkerheden.

Informationer

Informationsaktiver må ikke fjernes fra virksomheden uden fornøden autorisation. Det betyder, at IT-udstyr kun må tages med hjem, hvis der foreligger en tilladelse til det.

Kundedata må kun kopieres til bærbare medier, hvis der er et særligt arbejdsbetinget behov herfor.

Alle medarbejdere i virksomheden, og dennes samarbejdspartnere, har et ansvar for, at informationsudveksling sker på en forsvarlig måde i forhold til typen af informationer, der udveksles, og i øvrigt at overholde gældende lovgivning. Kryptering skal så vidt muligt anvendes ved informationsudveksling.

Passwords

Passwords er personlige og skal opbevares omhyggeligt. Hvis der er mistanke om, at et password er kendt af andre, skal det straks ændres.
Personlige passwords til virksomhedens IT-systemer må ikke anvendes ved adgang til "fremmede" websider, hvor der kræves et password.
Passwords må aldrig lagres eller overføres elektronisk i klartekst.

Udstyr

Brugerne skal instrueres i brugen af mobilt udstyr (bærbare computere, smartphones og tablets) samt om risikoen ved at anvende mobilt udstyr, herunder at mobilt udstyr skal

beskyttes mod fysisk tyveri fra eksempelvis biler og andre transportmidler.

Det skal sikres, at der bliver taget de nødvendige sikkerhedskopier af væsentlige informationer på bærbart udstyr. Som udgangspunkt bør data altid lagres på netværksdrevet.

Bærbare computere skal regelmæssigt tilsluttes netværket, så det sikres, at de regelmæssigt opdateres med den nødvendige beskyttelse mod skadevoldende programmer.

Forholdsregler ved sikkerhedsbrud

Hvis du bemærker ting, som kan være tegn på et sikkerhedsbrud, skal du altid kontakte IT-afdelingen – det er bedre at kontakte én gang for meget end én gang for lidt.
Generelt hvis din enhed bliver ramt:

1. Isoler straks enhed fra netværk eller sluk enhed
2. Giv besked til IT-afdelingen
3. Noter så mange oplysninger som muligt om det der førte til hændelsen
4. Afvent nærmere instruktioner fra IT-afdelingen

Hvad kan du ellers gøre?

Se også de andre pixibøger om mailsikkerhed, sikkerhed på Internettet samt sikkerhed på PC.

Hovedkontor

Rugbjergvej 10, 4623 Lille Skensved

Afdeling Sydsjælland

Grimstrupvej 155, 4700 Næstved

Afdeling Vestsjælland

Norvangen 3D, 4220 Korsør

Afdeling Jylland

Hjulmagervej 4A, 7100 Vejle

Telefon
+45 70 26 69 00

Mail
info@td-k.dk