IT-sikkerhedspolitik for ORGANISATION X

CyberPilot

IT-sikkerhedspolitik for ORGANISATION X

Disse politikker kan bruges som inspiration til egne IT-sikkerhedspolitikker, eller kopieres og implementeres i din organisation - det er helt op til dig. Vær blot opmærksom på at udskifte X med din egen organisations navn.
God fornøjelse! :-)

Mange venlige hilsener,
CyberPilot teamet

Formål

Sikkerhedspolitikken definerer rammerne for styring af informationssikkerhed i ORG X.

Gyldighed

Sikkerhedspolitikken gælder for alle ansatte i ORG X og al anvendelse og adgang til ORG Xs informationssystemer.

Målsætninger

- ORG X arbejder aktivt med styring af informationssikkerhed med det formål at sikre tilgængelighed, integritet og fortrolighed af ORG X's informationsaktiver, systemer og data.
- X tilstræber at efterleve ISO 27001:2013 / ISO27002:2013.
- X anvender en risikobaseret tilgang, hvor beskyttelsesniveauet og omkostningerne hertil skal være baseret på en forretningsmæssig risiko- og konsekvensanalyse som skal foretages minimum årligt.
- En it-sikkerhedshåndbog skal udarbejdes og løbende vedligeholdes. Denne håndbog skal indeholde beskrivelser af implementerede tiltag ift. informations-sikkerhed samt henvisninger til relevante politikker, retningslinjer og procedurer.
- X tilstræber at overholde relevant lovgivning – herunder eksempelvis GDPR.

- X tilstræber at overholde de indgåede aftaler med eksterne parter, herunder databehandleraftaler.

- X tilstræber at få udarbejdet en årlig erklæring – ISAE3402, ISAE3000, ISO-certificering etc.

- Denne informationssikkerhedspolitik skal evalueres på årlig basis.

Organisation og ansvar

- **Bestyrelsen** har det ultimative ansvar for informationssikkerheden i ORG X.

- **Direktionen** er ansvarlig for styringsprincipperne og delegerer specifikke ansvarsområder for beskyttelsesforanstaltninger, herunder ejerskab af informationssystemer.

- **Ejerskab** fastsættes for hvert kritisk informationssystem. Ejeren fastlægger hvorledes sikringsforanstaltninger anvendes og administreres i overensstemmelse med sikkerhedspolitikken.

- **IT-afdelingen** rådgiver, koordinerer, kontrollerer og rapporterer om status på sikkerheden. IT-afdelingen udarbejder hertil understøttende retningslinjer og procedurer.

- **Den enkelte medarbejder** er ansvarlig for at overholde sikkerhedspolitikken og er informeret herom i "IT-anvendelsespolitikken".

Dispensationer

Dispensationer til ORG Xs informationssikkerhedspolitik og retningslinjer godkendes af IT-afdelingen ud fra retningslinjer udstukket af direktionen.

Rapportering

- IT-afdelingen informerer direktionen om alle væsentlige sikkerhedsbrud.

- Status over dispensationer inkluderes i IT-afdelingens årlige rapport til direktionen.

- Direktionen behandler årligt sikkerhedsstatus og rapporterer til bestyrelsen herom.

Overtrædelse

Forsætlig overtrædelse og misbrug rapporteres af IT-afdelingen til HR-afdelingen og nærmeste leder.

Overtrædelse af informationssikkerhedspolitikken eller understøttende retningslinjer kan få ansættelsesretlige konsekvenser.