Retningslinjer for medarbejdernes IT-anvendelse i ORGANISATION X

Disse retningslinjer kan bruges som inspiration til egne retningslinjer, 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

X har fokus på at sikre tilgængeligheden, fortroligheden og integriteten af sine systemer og data. Derfor skal alle medarbejdere handle på en ansvarlig, etisk og lovlig måde.
Alle Xs medarbejdere, konsulenter og midlertidige ansatte er forpligtet til at administrere viden med omhu og diskretion, uanset om den er skriftlig, elektronisk eller verbal. Derfor skal håndtering af viden være i overensstemmelse med Xs informationssikkerhedspolitik samt følgende regler og principper.
For at sikre dette bliver medarbejderne i X løbende trænet og gjort opmærksomme på emner indenfor IT-sikkerhed og Persondataforordningen igennem kontinuerlig træning.

Disse retningslinjer fastlægger således de grundlæggende regler for medarbejdernes anvendelse af IT i X, men stiller samtidig krav til medarbejdernes løbende opmærksomhed og viden.

Regler og principper

1. Fortrolighed

Du skal håndtere alle Xs oplysninger med diskretion og omhu.
Du må under ingen omstændigheder tilgå eller anvende oplysninger, systemer eller netværk, som ikke er nødvendige for dit job.
Du må ikke dele fortrolige oplysninger med kolleger, konsulenter eller midlertidige medarbejdere, som ikke har et jobspecifikt behov for disse oplysninger.
Du må ikke dele fortrolige oplysninger med eksterne parter, medmindre det har et klart forretningsmæssigt formål. Samtidig skal den eksterne part have underskrevet en fortrolighedserklæring.

2. Adgangskoder, PIN-koder

Alle adgangskoder og PIN-koder er udelukkende personlige.
Du skal have en lang adgangskode på minimum 12 tegn, hvor der både benyttes store og små bogstaver samt tal.
Du skal logge af eller låse din IT-arbejdsstation (fx bærbar, PC, tablet, mobiltelefon), hver gang du forlader den.

Du må aldrig have passwords stående på opslagstavler, papir eller på harddisk/e-mail.

3. Fysiske rammer

Dit skrivebord skal altid være ryddet. Fortrolige oplysninger skal sættes i aflåste skuffer, skabe eller lignende for at undgå uautoriseret adgang.
Du skal samtidig være bevidst omkring synligheden af din PC-skærm. Du skal ikke have fortrolige og følsomme data åbne, når uvedkommende står bag dig, således at de kan overvære dine aktiviteter over skulderen.

4. Håndtering af udstyr og dokumenter udenfor Xs område

Hvis du bringer mobilt udstyr uden for Xs kontorer, skal det være sikret med en PIN- eller adgangskode, der sikrer en tilfredsstillende sikkerhed mod adgang fra uautoriserede personer.
Mobilt udstyr, dokumenter osv. skal altid medbringes som håndbagage ved flyrejser.

5. Udstyr og software

Alle anvendte IT-systemer, udstyr eller hukommelsesenheder skal være godkendt af X eller følge standarder, som er udstedt heraf. Du må aldrig tilslutte uautoriseret udstyr til arbejdsstationer eller netværk. Dette gælder også USB-nøgler og smartphones. Derudover må du kun installere eller downloade programmer, hvis du har fået tilladelse til det.
Software og udstyr, såsom computere, bærbare computere og mobiltelefoner, er Xs ejendom og skal behandles i overensstemmelse derefter. De må derfor ikke udlånes til andre (inklusive familiemedlemmer).
Du skal anvende Xs interne filserver til håndtering af data. Anvendelse af cloudbaserede tjenester såsom Google Drive, Dropbox, OneDrive etc. og webbaserede fildelingstjenester er kun tilladt i forbindelse med modtagelse af data fra eksterne parter. Det er ikke tilladt at uploade Xs data til disse tjenester.
Software skal altid bruges i henhold til de licensvilkår, som X har indgået.

6. Brugeridentitet

Brugerrettigheder skal respekteres. Anvend kun din egen bruger. Du må aldrig dele dine brugeroplysninger med andre (heriblandt din chef). Brug af IT-udstyr, såsom bærbare computere eller mobiltelefoner, efterlader digitale spor som kan have konsekvenser for Xs omdømme i samfundet.

7. Brug af e-mail, internet og SMS

Du bør minimere privat brug af internettet og e-mail på Xs udstyr. Gem det i en folder med en "Privat" etiket. Personfølsomt data må ikke sendes på e-mail.
Arbejdsrelaterede online-korrespondancer må under ingen omstændigheder foregå igennem anonymiserede kommunikationskanaler.
Det er strengt forbudt at bruge Xs e-mail konti, computere, tablets og mobiltelefoner til at besøge websteder med pornografisk, racistisk eller andet ekstremt og kriminelt indhold.
Afsenders e-mailadresse/nummer skal altid tjekkes før ukendte links og dokumenter åbnes.

8. Sikkerhedsovervågning og logning

X respekterer den enkelte medarbejders privatliv og overholder de danske love og bestemmelser, men logger al IT-anvendelse og kan i særlige situationer kræve adgang til en brugers e-mail konto eller andre oplysninger, der genereres og lagres af medarbejdere, konsulenter og midlertidigt personale.

9. Håndtering af persondata

Hos X er vi meget opmærksomme på at passe godt på og beskytte de personlige informationer, som vores kunder, medlemmer, medarbejdere og partnere har betroet os at varetage. Vi arbejder løbende med at udvikle og implementere sikre processer, som skal sikre en lovmæssig og sikker behandling af persondata.

Vi har derfor etableret følgende grundprincipper for behandling af persondata:

- Medarbejdere må kun tilgå persondata, som er relevant for deres arbejde og funktion
- Medarbejdere må kun dele persondata (f.eks. persondata tilsendt fra kunder eller partnere) med andre medarbejdere, hvis det er relevant for deres opgave og funktion
- E-mails indeholdende persondata bør slettes, når den relevante data er behandlet
- Medarbejdere må ikke opbevare persondata lokalt på it-udstyr eller i e-mail indbakken længere end højst nødvendigt. I stedet bør man anvende de relevante systemer, som er designet og implementeret til dette formål (f.eks. XXXX)
- Medarbejdere bør periodevist gennemgå både filer og mapper (både fysiske og digitalt) for at sikre, at de ikke indeholder persondata, som gemmes længere end højst nødvendigt.

10. Rapportér sikkerhedshændelser

Hvis du har mistanke eller er overbevist om sikkerhedsmæssige hændelser, så skal du indberette dette omgående til nærmeste leder og IT-afdelingen.

Eksempler på sikkerhedshændelser:

- Modtagelse af mistænkelige e-mails
- E-mails med persondata sendt til forkert modtager
- Bortkommet it-udstyr

Tøv endelig ikke med at kontakte den ansvarlige (XXX) hvis du mistænker noget – *hellere en gang for meget end en gang for lidt!*