SKABELON

VIRKSOMHEDENS   
TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER

*Dette er en skabelon til en beskrivelse af virksomhedens tekniske og organisatoriske sikkerhedsforanstaltninger. I skabelonen er der indsat eksempler på de tekniske og organisatoriske sikkerhedsforanstaltninger, en virksomhed kan have.*

*Det er vigtigt, at skabelonen tilpasses de sikkerhedsforanstaltninger, der er opstillet i den enkelte virksomhed.*

**ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER:**

|  |  |
| --- | --- |
| **EMNE** | **RETNINGSLINJER** |
| **Organisering:** | **Ansvarsperson for databeskyttelse:**  Der udpeges en person i organisationen, der har det overordnede ansvar for Datapolitikkens overholdelse, gennemgang, kontrol, tilpasning m.v. |
| **Uddannelse og introduktion:** | **Eksisterende medarbejdere:**  Alle medarbejdere, der behandler personoplysninger, undervises i alle relevante dele af Datapolitikken. |
| **Nye medarbejdere:**  Alle nye medarbejder introduceres for Datapolitikken og forpligtelserne heri så hurtigt som muligt efter ansættelsesforholdets tiltrædelse. |
| **Papir:** | **Papirudskrifter:**  Det efterstræbes at al behandling af personoplysninger i organisationen foregår digitalt, og at udskrift eller anden form for håndtering af personoplysninger i papirform begrænses i videst muligt omfang. |
| **Opbevaring af personoplysninger i papirform:**  I det omfang der opbevares personoplysninger (uanset typen af personoplysninger) i papirform, opbevares disse i aflåste og brandsikre skabe, hvor kun relevante personer har adgang/nøgler til. |
| **Makulering af papir:**  Minimum én gang hver 14. dag ryddes der op i alle skabe m.v. med papiroplysninger.  I det omfang, at der ikke længere er et formål med at opbevare oplysninger i papirform (eksempelvis fordi dokumenterne foreligger i digital form) makuleres dokumenterne i en krydsmakulator. |
| **Kontrol:** | **Stikprøvekontrol:**  Der føres løbende (minimum én gang i kvartalet) stikprøvekontrol med, at alle de organisatoriske sikkerhedsforanstaltninger overholdes i hele organisationen. |

**TEKNISKE SIKKERHEDSFORANSTALTNINGER:**

|  |  |
| --- | --- |
| **EMNE** | **RETNINGSLINJER** |
| **Teknisk beskyttelse mod uautoriseret adgang:** | **Beskyttelse mod digitale angreb:**  Alle IT-systemer og –enheder beskyttes mod uautoriseret adgang ved opsætning af de nødvendige sikkerhedsforanstaltninger, herunder:   * Firewall * Antivirus-foranstaltninger * Spamfiltre * Løbende opdatering af software |
| **Netværkssikkerhed:**  Alle netværk i organisationen er opsat med de nødvendige sikkerhedsforanstaltninger med henblik på beskyttelse mod uautoriseret brug og adgang. |
| **Sikkerhedskopiering:** | **Backup:**  Alle systemer i organisationen, hvor der opbevares personoplysninger, sikkerhedskopieres jævnligt, så al data kan gendannes i tilfælde af fejl. |
| **Fysiske personers adgang til IT-systemer:** | **Adgangsbegrænsning:**  Det sikres, at kun de medarbejdere, det er relevant for, har adgang til de IT-systemer, hvori der opbevares personoplysninger.  Der etableres et autorisationssystem, hvor hver enkelt medarbejder for et individuelt og unikt brugernavn til individuel brugerprofil (brugernavne genbruges aldrig, selvom medarbejderen er fratrådt).  Alle medarbejderes adgang til og brug af IT-systemer logges, så der til enhver tid er kontrol med brug og adfærd.  Når en medarbejder fratræder, slettes brugerprofilen straks. |
| **Adgangskoder:**  Det sikres, at kun den enkelte medarbejder kan få adgang til medarbejderens ”brugerprofil” i IT-systemet.  Alle medarbejdere har egen og individuel adgangskode.  Adgangskoden ændres minimum hver tredje måned og skal være ny i forhold til tidligere anvendte koder.  Der må ikke anvendes standardkoder.  Adgangskoden skal som minimum bestå af følgende:   * Ét stort bogstav * Ét tal   Alle arbejdsstationer låser efter 5 minutters inaktivitet og låses op igen med individuel skærmlås.  Det er forbudt at give tilladelse til, at brugernavn og adgangskode huskes – dette gælder for både hardware og software. |
| **E-mails:** | **Brug af sikker/krypteret mail:**  Der bruges altid sikker/krypteret mail ved fremsendelse af e-mails indeholdende personoplysninger om CPR-numre, strafbare forhold og særligt følsomme personoplysninger. |
| **Arkivering af e-mails:**  Alle mails, der indeholder personoplysninger og som er relevante at gemme, arkiveres uden for indbakken. |
| **Oprydning i indbakke, sendt post og slettet post:**  Der ryddes jævnligt op i mapperne indbakke, sendt post og slettet post, så der ikke gemmes mails med personoplysninger i disse mapper. |
| **Data på digitale enheder:** | **Opbevaring af data på enheder stillet til rådighed af organisationen:**  Der må alene opbevares personoplysninger på mobile enheder (telefoner, iPads, laptops, USB-stik m.v.), såfremt disse enheder er beskyttet med et sikkerhedsgodkendt krypteringsprogram. |
| **Tyveri af digitale enheder:**  Der udføres kontrol med alle digitale enheder tilhørende virksomheden, så alt indhold på enheden kan destrueres ved et eventuelt tyveri eller mistet enhed. |
| **Opbevaring af data på private enheder:**  Der må ikke opbevares eller flyttes personoplysninger på/til private enheder. |
| **Destruering af hardware:** | **Destruering/bortskaffelse af hardware:**  Al hardware destrueres og bortskaffes på sikker vis. |
| **Kontrol af tekniske sikkerhedsforanstaltninger:** | **Kontrol:**  Minimum én gang i kvartalet foretages der en afprøvning, vurdering og evaluering af de tekniske sikkerhedsforanstaltninger. |