IT-SIKKERHEDSPOLITIK FOR DESINO APS

1. INDLEDNING

Sikkerhedspolitikken skal til enhver tid understøtte virksomhedens værdigrundlag og vision samt demonstrere, at virksomheden har en seriøs holdning til sikkerhed for persondata, systemer og andre IT-aktiver.

Hensigten med sikkerhedspolitikken er endvidere at tilkendegive over for alle, som har en relation til virksomhed, at anvendelse af informationer og informationssystemer er underkastet standarder og retningslinjer.

Fastholdelse og udbygning af et højt sikkerhedsniveau er en væsentlig forudsætning for, at virksomheden fremstår troværdig, og for at fastholde denne troværdighed skal det sikres, at al information behandles med fornøden fortrolighed og at der sker fuldstændig, nøjagtig og rettidig behandling af godkendte transaktioner.

IT-systemer betragtes, næst efter medarbejderne, som virksomhedens mest kritiske ressource. Der lægges derfor vægt på driftsikkerhed, kvalitet, overholdelse af lovgivningskrav og på at systemerne er brugervenlige, dvs. uden unødigt besværlige sikkerhedsforanstaltninger.

Der skal skabes et effektivt værn mod IT-sikkerhedsmæssige trusler, således at vores image og medarbejdernes tryghed og arbejdsvilkår sikres bedst muligt. Beskyttelsen skal være vendt imod såvel naturgivne som tekniske og menneskeskabte trusler. Alle personer betragtes som værende mulig årsag til brud på sikkerheden; dvs. at ingen persongruppe skal være hævet over sikkerhedsbestemmelserne.

Tilsidesættelse af denne IT-politik kan få aftaleretlige, herunder ansættelsesretlige, konsekvenser for såvel medarbejdere, ledelse som leverandører. Ledelsen er pligtig at påse overholdelsen.

2. FORMÅL

Målene for virksomhedens IT-politik er at

- opnå høj driftsikkerhed med høje oppetidsprocenter og minimeret risiko for større nedbrud og datatab - TILGÆNGELIGHED
- opnå korrekt funktion af systemerne med minimeret risiko for manipulation af og fejl i såvel data som systemer - INTEGRITET
- opnå fortrolig behandling, transmission og opbevaring af data - FORTROLIGHED
- opnå en gensidig sikkerhed omkring de involverede parter - AUTENTICITET
- opnå en sikkerhed for gensidig og dokumenterbar kontakt - UAFVISELIGHED

alt under skyldig hensyntagen til den til enhver tid værende persondatalovgivning.

3. VIGTIGE GRUNDPRINCIPPER

3.1 FUNKTIONSADSKILLELSE

Funktionsadskillelse er det bærende kontrolprincip på såvel personligt som organisationsplan. Dette er sjældent praktisk fuldt ud muligt, blandt andet af hensyn til medarbejderens IT-færdigheder og -kompetencer. I det omfang, det er muligt, og opgaven således ikke er outsourcet til en databehandler, herunder et lønbureau eller en IT-supporteringsvirksomhed, er det ledelsens pligt at sikre, at alle nødvendige behandlingsskridt noteres med navn, dato og beskrivelse af behandlingen.

3.2 SIKKERHEDSFORANSTALTNINGER

Direktør, Martin Egesø, beslutter omfang og styrke af de sikkerhedsforanstaltning, der findes nødvendige at installere. Sådanne installeres af den IT-ansvarlige, hvilken funktion kan være outsourcet. Ledelsen varetager og formulerer administrative foranstaltninger ved nye tiltag og foranstaltninger, herunder udarbejdelse af retningslinjer og instrukser.

3.3 STYRING AF SIKKERHEDSHÆNDELSER

Martin Egesø skal løbende sikre og monitere eventuelle hændelser, der kan true sikkerheden, således at risikoen for databrud kan minimeres eller undgås.

Martin Egesø er opmærksom på pligten til at foretage indberetning af databrud. Ved databrud skal følgende iagttages.

Virksomheden skal foretage anmeldelse af sikkerhedsbruddet til Datatilsynet uden unødig forsinkelse, dog senest 72 timer efter, vi er blevet bekendt med bruddet.

Anmeldelsen skal foretages af direktør, Martin Egesø, som kontaktperson, og anmeldelsen skal mindst

- beskrive karakteren af bruddet, herunder forventet antal berørte og kategorierne af oplysninger,
- sandsynlige konsekvenser af sikkerhedsbruddet, og
- de foretagne foranstaltninger, der er truffet.

Derudover dokumenteres alle brud på persondatasikkerheden, herunder de faktiske omstændigheder ved bruddet, dets virkninger og de trufne, afhjælpende foranstaltninger.

Hvis bruddet indebærer en høj risiko for fysiske personer, underretter vi som udgangspunkt den unødig forsinkelse de registrerede om bruddet. Martin Egesø har ansvaret herfor.

3.4 DOKUMENTATION

Såfremt der skal udføres særlige, væsentlige sikkerhedsaktiviteter, skal disse planlægges, risikovurderes og dokumenteres.

4 ORGANISERING AF SIKKERHEDSARBEJDET

Martin Egesø har det overordnede ansvar for det IT-mæssige sikkerhedsarbejde. Som overordnet ledelse kan og skal han i fornødent omfang inddrage medarbejdere og samarbejdspartnere, der fungerer som databehandlere.

Martin Egesø har ansvaret for udformningen af IT-politikken, herunder opdateringer heraf.

5 MEDARBEJDERE - SIKKERHEDSBEVIDSTHED

Den enkelte medarbejder har pligt til at gøre sig bekendt med IT-sikkerhedspolitikken, herunder reglerne for opkobling udefra, hjemmearbejde m.v. således at vedkommende opnår en sikkerhedsbevidsthed. Den enkelte medarbejdere har yderligere pligt til straks ved mistanke eller konstatering af eventuelle sikkerhedsbrud at foretage indberetning heraf til ledelsen.

Medarbejderne skal løbende informeres om IT-sikkerhedspolitikken, herunder om deres pligter og rettigheder og om nødvendigt undervises nærmere heri.

6 STYRING AF AKTIVER

Virksomhedens IT-aktiver (computere, tablets og telefoner) skal identificeres og registreres med en ejer, der typisk vil være den daglige bruger heraf.

Den registrerede ejer af aktivet har ansvaret for

- at aktivet til stadighed ved placering, brug og forandring m.v. opfylder IT-politikken,
- at aktivet til stadighed er forsynet med en af den registrerede ejer selvvalgt og hemmelig kode
- at aktivet til stadighed er forsynet med tilstrækkelig og opdateret firewall og viruskontrol.
- at sensitive koder ikke lagres automatisk

Ethvert aktiv skal sikre og beskyttes mod uautoriseret adgang, misbrug eller ødelæggelse under transport eller ved opbevaring. Dette gælder også – og især – bærbare computere, tablets og mobiltelefoner.

Enhver medarbejder har pligt til at sikre, at alle fysiske dokumenter, der indeholder persondata, almindelige eller følsomme, opbevares utilgængelige for uvedkommende, herunder i skabe eller andre arkivalier, og at sådanne makuleres, når disse ikke længere benyttes eller der foreligger en sletteplig i øvrigt iht. virksomhedens persondata- og privatlivspolitik.

Det er tilladt for medarbejderne at benytte virksomhedens aktiver til privat brug.

6.1 HR-OPLYSNINGER

Alle persondata, herunder følsomme, kan alene tilgås af Martin Egesø, der har ansvaret for lønbogholderi. Disse oplysninger kan alene tilgås af de pågældende efter indtastning af valgt kode til systemet.

6.2 KUNDEDATA

Alene de medarbejdere, der har behov for persondata på kunder, eksempelvis den medarbejder, der konkret udfører arbejde for pågældende kunde, har adgang til disse data. Principielt set har alle medarbejdere dog adgang hertil i erkendelse af, at en medarbejder kan blive nødsaget til at overtage en konkret opgave for en anden medarbejder.

7 STYRING AF ADGANG – FYSISK

Alle følsomme persondata opbevares hos den herfor ansvarlige i aflåste skabe. Almindelige oplysninger opbevares på virksomhedens kontor. Begge findes på direktør, Martin Egesøs hjemmekontor.

8 E-MAIL- OG KOMMUNIKATIONSSIKKERHED

Ingen e-mails må indeholde persondata i emnefeltet, ligesom e-mail indeholdende følsomme persondata i videst muligt omfang skal fremsendes krypteret. Lønsedler og andre HR-relaterede oplysninger skal altid fremsendes krypteret, kodet eller med sikker post.

9 VERSION OG OPDATERING

Den hurtige udvikling af internettet betyder, at ændringer i IT-sikkerhedspolitikken kan blive nødvendige. Derfor kan og skal direktør, Martin Egesø foretage ændringer heri, såfremt det er nødvendigt. Enhver ændring skal meddeles de berørte pligtsubjekter, eksempelvis medarbejderne.

Denne IT-sikkerhedspolitik er senest ændret den 1. Maj 2018.