IT-SIKKERHEDSPOLITIK FOR AUTOFOKUS

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 ansættelsesretslige, 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

Ledelsen beslutter omfang og styrke af de sikkerhedsforanstaltninger, 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

Ledelsen skal løbende sikre og monitere eventuelle hændelser, der kan true sikkerheden, således at risikoen for databrud kan minimeres eller undgås. Ledelsen skal holdes orienteret fra medarbejderne, jf. pkt. 5.
• Ledelsen 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 direktøren 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 dokumenterer ledelsen 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 unødige forsinkelse de registrerede om bruddet. Ledelsen har ansvaret herfor.

3.4 DOKUMENTATION

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

4 ORGANISERING AF SIKKERHEDSARBEJDET

Ledelsen har det overordnede ansvar for det IT-mæssige sikkerhedsarbejde. Ledelsen kan og skal i fornødent omfang inddrage medarbejdere og samarbejdspartnere, der fungerer som databehandlere. Ledelsen har ansvaret for udformningen af IT-politikken, herunder opdateringer heraf, ligesom ledelsen udpeger den eller de personer, der skal have adgang til især følsomme persondata.

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 medarbejder 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 (software, data og fysiske enheder) skal identificeres og registreres med en ejer, der typisk vil være den daglige bruger heraf. Er der tale om en hosted løsning, skal der tages hensyn hertil i aftalegrundlaget med samarbejdspartneren, afhængigt af, om vedkommende optræder som databehandler.
Den registrerede ejer af aktivet har ansvaret for
• at aktivet til stadighed ved placering, brug og forandring m.v. opfylder IT-politikken,
• at aktivet ikke udsættes for særlig risiko, eksempelvis særlig usikre offentlige netværk m.v.
• at aktivet til stadighed er forsynet med en af den registrerede ejer selvvalgt og hemmelig kode, der SKAL fornys mindst hver 3. måned,
• at aktivet til stadighed er forsynet med tilstrækkelig og opdateret firewall og viruskontrol,
• at sensitive koder ikke lagres automatisk.
Den registrerede ejer skal føre en logbog over sine forpligtelser, herunder tidspunkter for forandring af koder. Ledelsen kan kræve dokumentationen fremvist med mindst 6 måneders mellemrum, medmindre der foreligger en konkret begrundet mistanke om misbrug eller sikkerhedshændelser.
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.
Bortskaffelse af aktiver, som indeholder eller kan give adgang til persondata og andre følsomme oplysninger, herunder fortrolig information af hvad art tænkes kan, skal ske efter aftale med og instruks fra ledelsen, der skal sikre, at aktivet lagres og dokumenteres, hvorefter bortskaffelse kan ske forsvarligt, eksempelvis ved destruktion, makulering eller definitiv sletning af data.
Det er tilladt for medarbejderne at benytte virksomhedens aktiver til privat brug.

7 STYRING AF ADGANG - ELEKTRONISK
Enhver elektronisk adgang til virksomhedens systemer kræver log-on-koder. Alle fysiske aktiver kræver korrekt indtastet kode indenfor 3 forsøg. Herefter blokeres der for adgang indtil Louise Neimann (marketing@autofokus.dk) har godkendt ny opsætning af adgang.
Forgæves log-on-forsøg med spærring skal registreres manuelt af Louise Neimann (marketing@autofokus.dk) med angivelse af dato, ejer af aktivet, jf. pkt. 6, samt de faktiske omstændigheder ved hændelsen.

7.1 HR-OPLYSNINGER
Alle persondata, herunder følsomme, kan alene tilgås af Louise Neimann (marketing@autofokus.dk) og Julie Rettig Pedersen (julie@optimize.dk), der har ansvaret for lønbogholderi henholdsvis virksomhedens daglige ledelse. Disse oplysninger kan alene tilgås af de pågældende efter indtastning af en af dem valgt kode til systemet.

7.2 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.

7.3 PRIVAT BRUG AF AKTIVER OG E-MAILS
Private e-mails skal være arkiveret i mappe "PRIVAT" og slettes straks ved arbejdsforholdets ophør, såfremt medarbejderen ikke forud herfor selv har gjort dette.
Arbejdsrelaterede, nødvendige, e-mails fra tidligere medarbejdere, der ikke i forvejen er arkiveret, overføres til virksomhedens hovedpostkasse og arkiveres i overensstemmelse med virksomhedens generelle håndterings- og privatlivspolitik. Øvrige e-mails slettes samtidig med arbejdsforholdets ophør, dog senest 1 måned herefter.
Enhver håndtering af fratrådte medarbejderes e-mail skal være færdiggjort senest 12 måneder efter fratræden. Selve e-mailadressen skal nedlægges senest 1 måned efter fratræden med henvisning til en anden.

8 STYRING AF ADGANG - FYSISK
Alle følsomme persondata opbevares hos den herfor ansvarlige i aflåste skabe. Almindelige oplysninger opbevares på virksomhedens kontor, der låses af udenfor normal arbejdstid.

9 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.
Al overførsel af information, herunder via e-mail, skal klassificeres i forhold til persondatalovgivningen, ligesom der skal foretages en konkret risikovurdering. Om nødvendigt kan brugen af begrebet "fortroligt" eller "hemmeligt" benyttes i emnefeltet til forsendelse og overførsel.

10 DRIFTSSIKKERHED, ANSKAFFELSE OG VEDLIGEHOLDELSE
Driftssikkerhed drejer sig om at opnå korrekt og sikker drift af de faciliteter og systemer, der behandler, herunder opbevarer, information og persondata. Heri indgår dokumentation af procedurer for drift, softwareinstallation samt styring af ændringer, der løbende forekommer, herunder opdateringer, som kan påvirke sikkerheden.
Der skal indføres sikkerhedsforanstaltninger, der kan opdage og forhindre data- og sikkerhedsbrud, eksempelvis forårsaget af malware.
Ligeledes skal der foretages løbende backup af data, ligesom der skat udarbejdes en backup-plan til brug for større sikkerhedsbrud.
Enhver anskaffelse med tilhørende installation og vedligeholdelse må alene ske fra en leverandør, der opfylder betingelserne i pkt. 11.

11 OUTSOURCING

Leverandører, der helt eller delvist står for drift af virksomhedens aktiver og systemer skal overholde virksomhedens IT-sikkerhedspolitik. Der skal være mulighed for at udøve effektiv kontrol hermed, ligesom leverandører skal kunne dokumentere deres overholdelse.
I forbindelse med outsourcing kan det blive nødvendigt at udarbejde en databehandleraftale, der I detaljer skal beskrive de sikkerhedskrav, som leverandøren skal leve op til.

12 VERSION OG OPDATERING

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