IT-sikkerhedspolitik for Forsikringsagenturet Optima Gruppen ApS Fremover (”Agenturet”)

Indhold

1. INDLEDNING

1.1. Formål

IT-systemer spiller en væsentlig rolle i Agenturets hverdag som kilde til information og middel til at kommunikere med medlemmer, medarbejdere og kunder. Formålet med denne IT- og informationssikkerhedspolitik (frem over "IT-sikkerhedspolitikken") er således at opstille minimumskrav for de sikkerhedstiltag, som Agenturet anser for nødvendige for at føre forsvarlig forsikringsmæglervirksomhed.

IT-sikkerhedspolitikken bygger på tillid til, at Agenturets medlemmer læser og efterlever politikken samt udviser generel ansvarlighed i brugen af deres IT-faciliteter.

1.2. Omfang

IT-sikkerhedspolitikken gælder for alle Agenturets medlemmer uanset medlems- eller ansættelsesform, herunder også eksterne samarbejdspartnere, der har adgang til medlemmernes systemer og data. IT-sikkerhedspolitikken omfatter alt brug af netværksbaserede systemer, IT-udstyr, der kobles på medlemmernes systemer eller anvendes erhvervsmæssigt, samt alle databærende medier og eventuelle papirarkiver.

2. ORGANISERING OG ANSVAR

2.1. Internt

Den enkelte forsikringsmægler har det overordnede ansvar for at tilsikre kontinuerlig overholdelse og udvikling af IT-sikkerhedspolitikken.

2.2. Eksternt

I overensstemmelse med gældende lovgivning skal der indgås skriftlige aftaler med alle eksterne IT-leverandører og samarbejdspartnere. Disse aftaler skal overholde kravene i gældende persondataregler og tilsikre garantier for tilstrækkelige organisatoriske samt tekniske sikkerhedsforanstaltninger. Sikkerhedsforanstaltningerne bør omfatte, men ikke begrænses til: kryptering, sikkerhedskopiering, fysisk samt teknisk adgangskontrol og aftalte kontrolbeføjelser.

3. FYSISKE, TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER

3.1. Fysisk adgangskontrol

Medlemmernes lokaliteter sikres med et adgangskontrolsystem udvalgt på baggrund af en risikovurdering. Det enkelte medlems kontorfaciliteter er aflåst uden for almindelig kontortid, og gæster bevæger sig ikke udenfor dedikerede områder uden at være ledsaget af en medarbejder.

3.2. Tab eller destruktion af udstyr

Mistet eller ødelagt udstyr indberettes hurtigst muligt til medlemmets IT-ansvarlige.

Før bortskaffelse eller udskiftning af IT-udstyr slettes alle data. Sletning skal til enhver tid ske i overensstemmelse med vejledninger udstedt af nationale datatilsyn samt under iagttagelse af, hvilke typer af personoplysninger og systemer IT-udstyret indeholdt eller havde adgang til i sin brugsperiode.

3.3. Autorisationer

Medlemmerne sikrer gennem deres IT-systemer at begrænse adgangen til fortrolige oplysninger og personoplysninger til det nødvendige personale.

3.4. Styring af netværk

Medlemmernes IT-systemer og daglige drift er i dag, i overvejende grad, afhængig af adgang til internettet. Styring samt sikring af medlemmernes netværk er derfor af særlig forretningsmæssig betydning. Som følge af netværkets betydning er det nødvendigt at regulere det enkelte medlems brug, samt overvågning.

For at undgå utilsigtet eller uautoriseret adgang er medlemmernes netværk sikret efter gældende standarder. Der er således etableret firewalls og løbende overvågning for at styre samt beskytte netværket.

Medlemmers trådløse netværk er beskyttet med password. Det enkelte medlem sikrer til stadighed, at adgangen er reguleret for at forhindre uvedkommendes adgang. Medlemmernes trådløse netværk opfattes som usikkert og bør ikke anvendes til fortrolige transaktioner eller kommunikation. Gæster kan få udleveret kodeord til et gæstenetværk og tilslutte eget udstyr.

3.5. Skadevoldende programmer (vira, orme, spy-, mal- samt ransomware)

Såfremt et medlem har mistanke om, at en enhed, et system eller netværk er inficeret, slukkes dette straks for at forhindre yderligere spredning. Efter enheden er slukket, tages der hurtigst muligt kontakt til det enkelte medlems IT-ansvarlig.

3.6. Sikkerhedskopiering og backup

Det enkelte medlem foretager systematisk sikkerhedskopieringer af netværksdrev og systemdrev.

4. MEDLEMMERS ADFÆRD OG BRUG

4.1. Etiske standarder

Medlemmernes netværk må ikke benyttes til besøg på hjemmesider, hvis indhold er af pornografisk, ekstremistisk eller diskriminerende karakter for så vidt angår race, køn, etnisk eller social oprindelse eller religion. Tilsvarende gælder ved brug af mail, mobile enheder eller databærende medier.

4.2. Password-politik

Alle medlemmer er ansvarlige for deres samt medarbejderes personlige adgangskode.

Ved enhver mistanke om, at et password er blevet kendt af uvedkommende personer, skal dette straks ændres og IT-afdelingen kontaktes. Ved gentagne forkerte loginforsøg vil brugerens adgang til det enkelte medlems IT-system blive midlertidigt lukket.

4.3. Lagring af information

Informationer skal lagres i det omfang, der er et arbejdsmæssigt behov herfor. Data indeholdende personoplysninger skal lagres i overensstemmelse med Agenturets datapolitik.

Det er ikke tilladt at kopiere, flytte eller lagre fortrolige data på bærbare medier, medmindre dette skriftligt er godkendt af IT-afdelingen.

4.4. Deling af informationer

Det er ikke tilladt at anvende fildelingstjenester eller netværksdrev til deling af informationer, medmindre dette skriftligt er godkendt af det enkelte medlem. Oplysninger må således kun videregives internt i Agenturet i det omfang det er strengt nødvendigt og ikke uden korrekt hjemmel.

4.5. Brug af mobilt udstyr samt hjemmearbejdsplads

Indholdet af nærværende politik er gældende for alt mobilt udstyr med adgang til medlemmets systemer og netværk eller indeholdende forretningsdata. Herunder bl.a. men ikke udtømmende: mobiltelefoner, tablets og bærbare computere.

Medlemmerne forpligter sig til at have et opdateret antivirusprogram og firewall på alle mobile enheder, som har adgang til medlemmets netværk og systemer. Såfremt hjemmearbejdspladsen er tilkoblet et trådløst netværk hos den ansatte, er man forpligtet til ved opsætning at sørge for at sikre dette bedst muligt, herunder ændre standardpassword og standardnavn på netværket.

Smartphones og tablet skal opbevares på betryggende vis og må ikke udlånes eller på anden vis overgives til andre. Fortroligt materiale må aldrig lagres på smartphones eller tablets. Smartphones og tablets med adgang til det enkelte medlems e-mail, netværk eller systemer skal være sikret med mindst en 4-cifret pinkode. Hvis en smartphone eller tablet med adgang til det enkelte medlems e-mail, netværk eller systemer bortkommer eller ødelægges, skal der straks ske underretning.

4.6. Databærende medier

Alt brug af databærende medier (CD'er, USB-sticks, print m.v.) er medlemmets eget ansvar.

Før databærende medier videregives eller genanvendes, skal indholdet slettes eller overskrives. Databærende medier indeholdende personoplysninger skal altid overskrives på en måde, så data-ene ikke kan genskabes.

5. DOKUMENTANSVARLIG OG VERSIONSSTYRING

Jakob Bjørn Mouritzen er til enhver tid ansvarlig for denne IT-sikkerhedspolitik.

Dokumentet revideres mindst én gang om året.

Dokumentet er senest revideret d.: 2. juli 2018