IT-sikkerhedspolitik

Indholdsfortegnelse

Introduktion

Konventum A/S beskytter den registreredes personoplysninger og har fastlagt retningslinjer, der beskytter den registreredes personoplysninger mod, at der sker uautoriseret offentliggørelse, og mod at uvedkommende får adgang eller kendskab til dem.

Kun de personer/ansatte hos Konventum A/S, der i kraft af deres jobfunktion har behov for de registreredes personoplysninger, har adgang hertil. Konventum A/S kontrollerer løbende, at der ikke sker uautoriseret adgang til de registreredes personoplysninger.

Mål

Virksomheden ønsker at opnå:
- Fortrolighed i håndtering af persondata.
- Et højt sikkerhedsniveau for adgang til persondata.
- Dokumentation af persondata i overensstemmelse med kravene i persondataforordningen.
- Høj driftssikkerhed og minimal risiko for større nedbrud og tab af data.
- Et image som en virksomhed, der demonstrerer kvalitet og sammenhæng i brugen af IT og håndtering af data.

Sikkerhedsforanstaltninger

Den IT-ansvarlige beslutter i samarbejde med øvrige ledelse omfanget og styrken af de sikkerhedsforanstaltninger, som det findes nødvendigt at installere. Dette udformer sig både i tekniske installationer og formulering af administrative beslutninger (retningslinjer og personalepolitik m.v.).

Risikovurdering

Virksomheden vurderer løbende de tekniske foranstaltninger og politikker ud fra eventuelle hændelser såvel som kendte nye trusler og sårbarheder, der kan true sikkerheden og virksomhedens generelle risikobillede.

Dokumentering

Virksomheden har udarbejdet skriftlige procedurer og dokumentation for adgangsforhold til og brugen af virksomhedens IT-systemer (herunder adgang til persondata).

Leverandørforpligtelser

Leverandører, der helt eller delvist står for drift af virksomhedens systemer, skal overholde virksomhedens krav til it-sikkerhed.

I forbindelse med at der bliver indgået en kontrakt om outsourcing eller databehandling, skal der udarbejdes en databehandleraftale, der i detaljer beskriver de sikkerhedskrav, som leverandøren skal leve op til.

Virksomheden stiller endvidere krav til leverandører om at de kan levere en revisionserklæring, der dokumenterer, at it-sikkerheden er i orden i henhold til revisionsstandard 3411, type B.

Beredskabsplaner

Virksomheden har udarbejdet beredskabsplaner for hhv.:
- Strømafbrydelse
- Netværk
- Servere
- Backup
- Databrud

Tekniske foranstaltninger

Fysisk sikkerhed

Adgangsforhold
Virksomheden benytter sig af et elektronisk smartkey-system og kan således styre adgangsforhold på personniveau samt dokumentere adgangsforhold til lokaler og andre relevante installationer (skabe m.v.).

Videoovervågning:
Virksomhedens fysiske område (udendørs arealer) er videoovervåget. Videoovervågningen sker med det formål at kunne skabe tryghed og sikring imod indbrud og hærværk på virksomhedens og gæsternes ejendele (køretøjer m.v.), samt for at kunne dokumentere og videregive eventuelle strafbare forhold til politiet.

Følsomme oplysninger ved betaling
Ved indtastning af dankort/kreditkort-oplysninger ved online betaling, sker dette altid på en krypteret side, ligesom transmission af data sker krypteret (i henhold til krav fra PBS). Konventum har på intet tidspunkt adgang til følsomme dankort/kreditkort-oplysninger.

Hjemmesideformularer
Der anvendes kryptering (https) ved brug af formularer på virksomhedens hjemmeside.

Logning
Virksomheden logger adgangsforhold til IT-systemer og filer på virksomhedens netværk samt forsøg på udefrakommende hackerangreb (DDOS-angreb, sårbarhedsudnyttelser etc.).

Konventum A/S efterlever desuden den danske terrorlovgivning og fører derfor aktiv logning med brugen af det trådløse netværk, som Konventum A/S stiller til rådighed for deres gæster.

Firewall
Virksomhedens systemer og netværk er beskyttet af en redundant "2nd Generation Firewall".

Virusbeskyttelse
Virksomheden benytter sig af antivirus beskyttelse på alle lokale arbejdsstationer og servere samt antivirus og antispam filter på virksomhedens mailserver.

Patch management
Virksomheden benytter sig af patch management for at sikre at alle arbejdsstationer altid indeholder de nyeste patches og Windows opdateringer til computerens styresystem og software.

Backup
Virksomheden har sikret backup af alle kritiske systemer og data. Backup foretages både lokalt samt til ekstern backup-samarbejdspartner.

Ekstern backup er krypteret og opfylder ISO27001 og ISO22301 standarderne.

Reparation, service og skrotning af dataudstyr
Reparation og service af dataudstyr foregår internt i huset af egne IT-medarbejdere.

Skrotning af IT-udstyr sker via fast samarbejdspartner, som sikrer korrekt datasletning.

Personalepolitik

Konventum A/S har udarbejdet retningslinjer til virksomhedens medarbejdere for brugen af IT.

Dette inkluderer, men er ikke begrænset til:

- Retningslinjer for brug af virksomhedens IT-værktøjer.
- Procedurer for udskiftning af adgangskoder.
- Procedurer for affaldssortering og makulering af dokumenter med persondata.
- Procedurer for håndtering af rekrutteringsprocessor og dokumenter.
- Procedurer for håndtering af persondataoplysninger i systemer.
- Procedurer for opbevaring af fysiske papirer og mapper i henhold til dansk regnskabslovgivning og persondataforordningen.