WOLFF SVENDSEN A/S

SIKKERHEDSPOLITIK

For virksomheden:

Wolff Svendsen A/S
CVR. nr. 25332601
Industrivænget 38
3400 Hillerød

(herefter omtalt "Virksomheden")

Senest revideret 29. juni 2018

Dataansvarlig:

Stine Green Andersen

1. GENERELT

1.1. Denne Sikkerhedspolitikken er den overordnede ramme for IT-sikkerheden i Virksomhedens informationsbehandling generelt, og skal til enhver tid understøtte Virksomhedens værdigrundlag og vision samt de strategiske mål, der er i IT-strategien.

1.2. Sikkerhedspolitikken og Persondatapolitikken, der indeholder de konkrete retningslinjer om IT-sikkerhed, skal være tilgængelig for alle medarbejdere i Virksomheden.

1.3. Sikkerhedspolitikken er udarbejdet ud fra kravene hertil i EU Persondataforordningen.

2. FORMÅL

2.1. Det er en vitalt interesse for Virksomheden, at informationer behandles sikkerhedsmæssigt forsvarligt, idet informationer og informationssystemer, herunder netværk og telefoni, er særdeles vigtige for Virksomheden.

2.2. Sikkerhedspolitikken definerer den overordnede beskyttelsesramme af Virksomhedens personoplysninger og andre fortrolige oplysninger, og sikrer hermed at oplysningerne bevarer deres fortrolighed, integritet og tilgængelighed.

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

2.4. Fastholdelse og udbygning af et højt sikkerhedsniveau er en væsentlig forudsætning for, at Virksomheden fremstår troværdig.

2.5. For at fastholde Virksomhedens troværdighed skal det sikres, at information behandles med fornøden fortrolighed og at der sker fuldstændig, nøjagtig og rettidig behandling af godkendte transaktioner.

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

2.7. Der skal skabes et effektivt værn mod IT-sikkerhedsmæssige trusler, således at Virksomhedens 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.

2.7.1. Målene er derfor, at:

- opnå høj driftssikkerhed 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

2.8. Sikkerhedspolitikken skal danne grundlag for at forebygge og begrænse skader til en, for Virksomheden, kendt og accepteret størrelse samt sikre fortsat it-drift efter et sikkerhedsbrud.

2.9. Regler og retningslinjer fra Sikkerhedspolitikken skal løbende indarbejdes i de relevante gældende regler på personalepolitikkens område.

3. SIKKERHEDSPOLITIKKENS OMFANG

3.1. Virksomhedens sikkerhedskoncept omfatter følgende:

- Nærværende Sikkerhedspolitik,
- Intern dokumentation ved brud på persondatasikkerhed, og
- Intern persondatapolitik, der indeholder de konkrete retningslinjer om IT-sikkerhed.

4. GRUNDLÆGGENDE PRINCIPPER

4.1. Funktionsadskillelse

4.1.1. Virksomheden har et grundlæggende princip om funktionsadskillelse. Det vil sige, at kun de nødvendige og relevante personer får adgang. Direktionen beslutter hvem, der skal have adgang til hvilke ressourcer og hvornår.

4.1.2. Hver enkelt medarbejder/bruger har hver sit login, så Virksomheden kan begrænse adgangen og kontrollere evt. misbrug.

4.2. Sikkerhedsforanstaltninger

4.2.1. Virksomheden har gennemført passende tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes, ændres eller forringes samt mod, at de kommer til uvedkommendes kendskab eller misbrug. Direktionen beslutter omfanget og styrke af de sikkerhedsforanstaltninger, som det findes nødvendigt at installere. Den it-ansvarlige installerer de tekniske foranstaltninger, mens direktionen står for formuleringen af de administrative foranstaltninger og retningslinjer, som fremgår af Virksomhedens Persondatapolitik.

4.2.2. Virksomheden har et clean-desk-princip. Det betyder, at medarbejderne er instrueret i at rydde alle papirer, dvd'ér, usb-nøgler og andre medier væk, når medarbejderen forlader sit skrivebord. Det skal være med til at mindske risikoen for at personoplysninger mistet. Herudover er medarbejderne instruereret i at låse sin computer og slukke for sin skærm, når vedkommende forlader sit skrivebord.

4.2.3. Virksomhedens IT-infrastruktur, lokaler og IT-udstyr er beskyttet mod at uautoriseret fysisk adgang samt fysiske skader og uønskede hændelser. Alle computere, mobiltelefoner mv. har adgangskoder, og de fysiske lokaler af aflåst.

4.2.4. Adgangen til at udføre handlinger i Virksomhedens IT-systemer er beskyttet af adgangskontroller. Systemerne har til formål at sikre mod uautoriserede ændringer, ordrer, fejl og svindel.

4.2.5. Alle indkøb, udvikling og implementering af nye systemer foregår kontrolleret for at undgå unødvendige risici for Virksomhedens oplysninger. Når løsninger implementeres, skal sikkerhedsovervejelser altid indgå som en integreret del af processen. Systemerne skal derfor sikre, at de krav til sikkerhed bliver identificeret i forbindelse med udarbejdelse af kravspecifikation ved anskaffelse af et nyt system.

4.3. Styring af sikkerhedsforanstaltninger

4.3.1. Alle medarbejdere og øvrige brugere er gjort bekendt med forretningsgangene for rapportering af forskellige typer hændelser og svagheder, der kan have indflydelse på sikkerheden for Virksomhedens aktiver. Væsentlige sikkerhedshændelser og svagheder skal hurtigst muligt rapporteres til Stine Green Andersen.

4.3.2. Virksomheden skal løbende følge meddelelser og opdateringer fra systemleverandører for at begrænse evt. hackerangreb.

4.4. Dokumentation

4.4.1. Virksomheden har udarbejdet skriftlige procedurer for alle væsentlige sikkerhedsaktiviteter, hvilket fremgår af den interne Persondatapolitik. Herudover har Virksomheden indgået skriftlige databehandleraftale med alle databehandlere.

4.4.2. Virksomheden vil iværksætte sikkerhedsundersøgelser/risikoanalyser i det omfang Virksomheden finder det nødvendigt.

5. GYLDIGHED

5.1. Sikkerhedspolitikken er gældende for alle Virksomhedens informationsrelaterede aktiviteter, uanset om disse udføres af ansatte i Virksomheden eller af samarbejdspartnere.

6. MEDARBEJDERE

6.1. Den enkelte medarbejder har ansvaret for, at overholde nærværende Sikkerhedspolitik, samt at rapportere om eventuelle sikkerhedsnedbrug eller mistanke herom til Stine Green Andesen.

7. BEREDSKABSPLAN

7.1. Virksomheden har implementeret passende og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes, ændres eller forringes samt mod, at de kommer til uvedkommendes kendskab eller misbrug. Brud på datasikkerheden er mindsket ved en veltilrettelagt fysisk sikring og overvågning af bygningen, tekniske installationer og it-udstyr.

7.2. Såfremt sikkerhedshændelser indtræffer, hvad enten det er et virusangreb, at oplysninger er faldet i de forkerte hænder, eller at en tredjepart har fået uautoriseret adgang, skal Virksomhedens beredskab iværksættes, så snart det vurderes at være nødvendigt.

7.2.1. Konstaterede it-sikkerhedsmæssige brud på eller trusler mod IT-sikkerheden skal registreres og dokumenteres, og alle væsentlige brud skal rapporteres til Stine Green Andersen til vurdering samt til den løbende opsamling af sikkerhedsproblemer til brug for revurdering af IT-sikkerheden. Den enkelte medarbejder har en pligt til at følge nedenstående handlingsplan og samtidigt dokumentere bruddet ved brug af vedlagte **bilag 1**. Konstateringen skal anmeldes til Stine Green Andersen hurtigst muligt og senest efter 5 timer. Medarbejderen er oplyst om, at Virksomheden kan have en pligt til at anmelde bruddet overfor Datatilsynet indenfor 72 timer, hvilket er årsagen til sagens hastende karakter.

7.2.2. Handlingsplan:

Nr.	Handling	Tid
1	**Vurder situationen** Vurder situationen. Hvis der er risiko for, at data kan blive ødelagt eller skadet, afbrydes internetforbindelsen.	Start: Slut:
2	**Luk systemer** Vurder, om der er behov for at lukke systemer for at undgå spredning af angrebet. Informer relevante systemejere, brugere mv.	Start: Slut:
3	**Iværksæt undersøgelse** Iværksæt en undersøgelse af angrebet. Kontakt Stine Green Andersen.	Start: Slut:
4	**Skift adgangskoder** Vurder, om adgangskoder bør skiftes.	Start: Slut:
5	**Aktiver ekstra systemlogning** Vurder, om der bør iværksættes ekstra logning af systemer og netværk for at opklare og indsamle beviser om hændelsen.	Start: Slut:
6	**Kontakt leverandører** Kontakt leverandørerne, hvis de ramte områder driftes eksternt.	Start: Slut:
7	**Kontakt myndigheder** Vurder, om der skal foretages politianmeldelse, og om der er andre myndigheder som bør kontaktes, f.eks. ødelæggelse af persondata.	Start: Slut:
8	**Informer interessenter** Eventuelle øvrige interessenter informeres.	Start: Slut:

7.2.3. Stine Green Andersen fører tilsyn med overholdelsen af Sikkerhedspolitikken og de herunder fastsatte IT-sikkerhedsbestemmelser. Tilsynet foregår ved stikprøvekontroller. En gang årligt foretages en risikovurdering og herunder en vurdering af, om der skal ske ændring af de gældende it-sikkerhedsregler og tilhørende procedurer.

8. SANKTIONERING

8.1. Medarbejdere, der bryder nærværende Sikkerhedspolitik, kan straffes disciplinært. De nærmere regler om dette er fastsat i Virksomhedens Persondatapolitik.

9. AJOURFØRING

9.1. Denne Sikkerhedspolitik ajourføres årligt. Den er senest revideret den 29. juni 2018.