Søndergaard & Sønner A/S
IT-politik

IT-politik Søndergaard & Sønner A/S

Registrering af data
De data der registreres hos Søndergaard skal leve op til persondataforordningen, jvf vores nedskrevne politikker.

Data registreres i Navision udelukkende af hensyn til administrativt at kunne håndtere virksomhedens formål, nemlig at drive handel med cykeltilbehør og reservedele.

Herudover organiseres adgang til data således at så få medarbejdere som muligt har adgang til personfølsomme data.
Se mere herom i Persondata beskyttelses politik omkring personale, kunder og leverandører.

Det er ikke tilladt at gemme særligt personfølsomme data på PC ens harddisk og andre flytbare medier.

Hvis man f.eks. har modtaget ansøgninger o.l. på mail, skal man sørge for at slette disse når ansættelsesproceduren er færdig.

Persondata der ikke er nødvendige for virksomhedens virke må ikke registreres.

Beskyttelse af data.
Alle fysiske enheder, f.eks. PC'er, tablets, mobiltelefoner og virksomhedens servere skal være beskyttet af password eller kode eller anden form for beskyttelse, der skal sikre enhederne mod uønsket brug, passwords skiftes 1 gang årligt i forhold til virksomhedens servere.

Virksomhedens fællesdrev er organiseret og beskyttet ud fra et need to know princip.
Personaledata gemmes på et specielt drev hvortil kun autoriseret personale har adgang.

Virksomhedens servere er i et aflåst skab. Sikring af data og backupsystemer er opbygget i samarbejde med RIT A/S, vi reviderer løbende procedurer og sikkerhed sammen med RIT A/S.

Netværk.
Alle virksomhedens netværk herunder også trådløse netværk er beskyttet af kode.
Vi har 3 trådløse netværk.
1. gæstenetværk som kun giver adgang til internettet.
2. mobil og tablet netværk der giver adgang til mail server.
3. Bærbar pc netværk der giver adgang til alt hvad medarbejderen i øvrigt har adgang til.

Adgangskode til mobile netværk skiftes 1 gang om året.

Virksomhedens lokaler.
Virksomhedens lokaler er sikret med hegn, lås og alarmsystem, vi har gennemført sikring af lokalerne i samarbejde med Falck, G4S og Verisure, i øjeblikket samarbejder vi med Verisure.
Vores forsikrings selskab har efterfølgende fysisk besigtiget og godkendt sikringen af lokaler.

1. Retningslinjer for anvendelse af IT-systemer udarbejdet med hjælp fra RIT A/S:

Dette er et kortfattet sammendrag af de retningslinjer for god IT-opførsel, som vi forventer af vores personale. Retningslinjerne omhandler forhold, man som it-bruger skal være opmærksom på omkring hensigtsmæssig og sikkerhedsmæssig forsvarlig anvendelse af firmaets netværk, systemer og data.

Anvendelse af IT systemer hos Søndergaard skal foregå med omtanke og til løsning af opgaver i forbindelse med arbejde.

Login
Når man som bruger har modtaget loginnavn og password, der giver adgang til netværket og dets servere, er man ansvarlig for alle handlinger, der udføres under brug af dette loginnavn. Udlån eller deling af personligt loginnavn/ password med andre er ikke tilladt.
Hvis der er mistanke om at andre har kendskab til ens password, skal Erik eller Frank straks kontaktes. På lageret og i varemodtagelsen giver det mening at have et fælles login for medarbejdere, på disse steder gælder at login ikke må deles med udenforstående.

Pas på din PC!
Hvis firmaet stiller en PC til rådighed, skal dette værktøj betragtes som et arbejdsredskab og må kun indeholde oplysninger som har relation til det daglige arbejde.
Hvis din PC bliver stjålet skal Erik eller Frank kontaktes omgående og der skal indgives politianmeldelse. Hvis pc'en er stjålet fra ens egen bil eller privat husstand, skal du være opmærksom på at firmaet ikke har forsikring på den. Lad være med at efterlade PC'en på steder, hvor den er særlig udsat for tyveri. Det tillades fx ikke at du opbevarer PC'en i bilen natten over.

Søndergaards IT-systemer må ikke anvendes, så det kan skade selskabets omdømme.

Følgende aktiviteter er ikke tilladt:

1. Sletning, eller modifikation af andres filer og/eller data uden der på forhånd er givet tilladelse.
2. Enhver form for uautoriseret overlagt handling, der kan ødelægge eller afbryde den normale funktion af et system, ændre dets normale funktion eller få det til at fejle er en overtrædelse, uanset hvor systemet befinder sig, og hvor længe handlingen står på.
3. Installation af software, der ikke har arbejdsmæssig relevans, samt software hvor firmaet ikke ejer den nødvendige licens, hvis der er tvivl, skal systemadministratoren godkende det ønskede software.
4. Kopiering af copyright materiale, fx tredje parts programmer, uden tilladelse fra ejeren eller uden legal licens.

2. Retningslinjer for brug af elektronisk post.
Når en bruger sender elektronisk post er brugerens navn såvel som Søndergaards adresse inkluderet. Den enkelte bruger har derfor ansvaret for al post, der er afsendt via det pågældendes loginnavn

Firmaets e-mail adresse er til firma relaterede opgaver og må kun i begrænset omfang videregives til privat brug, hvilket vil sige at der ikke må tilmeldes services fra for eksempel, konkurrencer, dating, eller andre ikke relaterede services.

E-mail ejes 100% af firmaet, og er således ikke privat.

Dette betyder, at følgende ikke er tilladt:

1. Forfalskning (eller forsøg på forfalskning) af elektronisk post.
2. at læse, slette, kopiere andres elektroniske post.
3. at afsende generende, obskøne eller truende meddelelser.
4. at sende junkmail, kædebreve (Spam) eller lignende former for meddelelser.

Hvis vi skal undgå uautoriseret adgang til vores IT systemer, skal du være ekstra opmærksom, når du modtager mails.

Inden du åbner mailen skal du sikre dig følgende:

1. Kender du afsenderen? Hvis ikke vær opmærksom.
2. Alle mails der starter med HI eller Dear friend uden navn – Slettes med Shift+delete.
3. Alle mails på engelsk eller dårligt formuleret dansk skal du være ekstra opmærksom på.
4. Alle mails indeholdende links eller filer skal du være ekstra opmærksom på.
   Er du det mindste i tvivl så tast shift + delete eller spørg Erik (hvis Ikke Erik er der så kontakt Frank)
   Suspekte mails må under ingen omstændigheder videresendes.

3 Netværkssikkerhed

Netværket benyttes udelukkende til jobrelaterede formål.
Netværket må ikke misbruges

4 Mobiltelefoner

Pas på din mobiltelefon!
Firmaet stiller i det omfang det er nødvendigt en mobiltelefon til rådighed.

Hvis telefonen bliver stjålet eller tabt skal Finn V. eller Frank straks kontaktes og telefonen bliver lukket omgående, hvis dette sker i weekend kontaktes telefonileverandøren for lukning af nummer og services, straks efter weekend kontaktes Finn V. eller Frank som sørger for det fornødne.
Ved tyveri skal der indgives en politianmeldelse omgående, således vi kan dokumentere over for teleselskab samt forsikring at telefonen er uden for vores rækkevidde.

Nummeret vil være spærret i kort tid indtil nyt SIM kort er fremskaffet fra teleselskab.

Hvis din mobiltelefon bliver stjålet skal Finn V. eller Frank kontaktes omgående og der skal indgives politianmeldelse. Hvis mobiltelefonen er stjålet fra ens egen bil eller privat husstand, skal du være opmærksom på at firmaet ikke har forsikring på den, da det ikke kan betale sig pga. selvrisiko og præmiestørrelse.

Mobiltelefonen kan repræsentere en stor værdi, så pas på den, og lad være med at efterlade mobilen på steder, hvor den er særlig udsat for tyveri. Det tillades fx ikke at du opbevarer mobiltelefonen i bilen natten over.

5. Andet
Der gøres opmærksom på, at der ved brug af IT-systemerne løbende foretages forskellige former for registrering af aktiviteterne af hensyn til opklaring af fejl, sikring af driftsstabilitet, sikring mod virus, spam m.v.
Elektronisk post er underkastet de samme fortrolighedsregler som almindelig post (brevhemmeligheden). Brugere af elektronisk post skal imidlertid gøres bekendt med, at denne form for post kan komme til andres kendskab ved systemfejl, fejl-adressering, eller såfremt en systemadministrator af tekniske årsager er nødt til at foretage en nøjere gennemgang af, hvad der går ind og ud af et konkret system.
Ved mistanke om misbrug eller uregelmæssigheder, kan firmaet gå ind og gennemgå mail korrespondance og internet brug.
Systemadministratorer og andre systemmedarbejdere er underkastet tavshedspligt. Det gælder imidlertid ikke alle andre potentielle modtagere af fejldistribueret post.
Firmaet forbeholder sig ret til at ændre dette dokument, uden varsel hvis det skønnes nødvendigt.

6. Brud på regler for IT-politik
En overtrædelse af denne IT-politik kan i værste fald medføre afskedigelse, idet overtrædelse sidestilles med misligholdelse.
En overtrædelse af forbuddet mod kopiering og/eller distribution af kopier kan medføre ansvar om erstatningspligt efter ophavsretsloven – ikke alene for den enkelte medarbejder men efter omstændighederne også for virksomheden.

Teknisk udstyr

7. Computer
Hvis man har bærbar PC.
Virksomhedens PC er kun til firmarelateret software. Har man privat installeret software såsom spil, som har forårsaget skade/problemer kan virksomheden i grove tilfælde gøre medarbejderen ansvarlig for den skade medarbejderens adfærd har forvoldt virksomheden.
Det er også medarbejderens ansvar, at der til enhver tid er opdateret antivirus software på PC'en.
I Pad som er udleveret af virksomheden er underlagt samme regler som computere.

8. Mobiltelefon
Vi har følgende regler vedr. brug af mobiltelefoner:

1. Vis hensyn med ringetoner og især højden af dem. Tag hensyn til dine kolleger og omgivelser generelt.
2. Husk at sætte mobiltelefon på lydløs under møder!
3. Sørg for at have en imødekommende og professionel velkomsthilsen på mobiltelefonsvareren.
4. Mobiltelefonen må bruges i henhold til den ansættelsesaftale der er indgået med den enkelte medarbejder.
5. Private mobiltelefoner må kun i begrænset omfang benyttes i arbejdstiden og må på ingen måde forstyrre arbejdet. Dette gælder ligeledes sms.

9.Slutning
Denne IT politik gælder fra 08.12.2017. Hvis du oplever at IT politikken er til hindring for dig i dit daglige arbejde, så tag det op med Erik, Henrik eller Frank, så vurderer vi om vi kan tilpasse politikken således, at du kan arbejde optimalt.