Forenede
Fordi der er forskel

Forenede Holding A/S
2860 Søborg
(+45) 39 55 56 01
forenede.dk
CVR: 36036656

Informationssikkerhedspolitik

Version	1.4
Dato:	Februar 2023
Ejer:	Head of group IT - Jacob Riis-Jacobsen
Godkendt:	Lars Folkmann

Formål

Formålet med denne informationssikkerhedspolitik er følgende:

- At sikre, at brugen af IT-systemer og data til enhver tid er i overensstemmelse med lovgivningen og indgåede aftaler med kunder og samarbejdspartnere.
- At sikre, at fornødne tekniske sikkerhedsforanstaltninger er tilstede.
- At sikre, at medarbejdere hos Forenede besidder den nødvendige viden til efterlevelse af denne informationssikkerhedspolitik.

Anvendelsesområde

Denne informationspolitik er gældende for alle ansatte og konsulenter i Forenede koncernen (herefter benævnt "Forende") samt ansatte hos leverandører med adgang til Forenedes IT-systemer. Dokumentet omfatter alle IT-systemer hos Forenede og alle typer information, uanset hvordan informationen opbevares eller behandles.

Sikkerhedsniveau

Relevante trusler, fejl og uheld skal forebygges, opdages og korrigeres. Det skal sikres, at virksomhedens drift til stadighed kan opretholdes, og at konsekvenserne af eventuelle sikkerhedsbrud reduceres til et minimum. IT afdelingens sikkerhedstiltag iværksættes under hensyntagen til såvel målet om et højt sikkerhedsniveau som effektive driftsbetingelser.

Sikkerhedsniveauet tager udgangspunkt i følgende principper:

- fortrolighed - sikre, at ingen uvedkommende har læst indholdet
- integritet - sikre, at ingen har ændret indholdet
- tilgængelighed - sikre, at systemer samt data er tilgængelige
- autencitet - sikre, at datas ophav er ægte
- uafviselighed - sikre, at der forefindes dokumentation for eksempelvis en transaktion

Adgang

Der er fastsat overordnede retningslinjer for, hvilke brugere der må få adgang til systemer. IT-afdelingen har det overordnede ansvar for den udførende del (brugeradministration og autorisation af brugere).

Eksterne leverandører kan få adgang til Forenedes IT-systemer eller dele heraf, såfremt der foreligger en skriftlig aftale, hvori leverandøren forpligter sig til at overholde den til enhver tid gældende sikkerhedspolitik.

Brugere må kun autoriseres til anvendelser, som de har behov for. IT-afdelingen foretager, i samarbejde med systemejeren, kvartalsvis kontrol af, at de tildelte adgangsrettigheder fortsat er arbejdsmæssigt begrundede. Fælles brugerkonti tillades ikke i forbindelse med adgang til personoplysninger.

I forbindelse med fratrædelse skal nærmeste leder træffe beslutning om overflytning af eventuelt personligt opbevarede data fra den fratrædende medarbejder. Senest på fratrædelsesdagen skal IT-afdelingen inddrage adgange til systemer m.v. efter information fra nærmeste leder.

Ved forsøg på uretmæssig adgang bliver adgangen til IT-systemerne spærret efter 3 forsøg. Passwords skiftes hver 3. måned og der er opsat et niveau for kompleksiteten for passwords på minimum 8 karakterer indeholdende specialtegn, store og små bogstaver samt tal. Systemet er, for at sikre unikke passwords, opsat til at huske de 10 sidste passwords.

Ved mistanke om forsøg på uretmæssig adgang, har enhver medarbejder hos Forenede pligt til at indberette dette til nærmeste leder eller til IT afdelingen.

Persondata

Definitioner

- Almindelige persondata
    - Navn, adresse, telefonnummer, e-mail mv.
- Personnummer
- Følsomme persondata
    - Helbredsoplysninger
    - Oplysninger om fagforening, politiske forhold m.v.
    - Oplysninger om biometriske og genetiske forhold
    - Oplysninger om race og etnisk oprindelse
    - Oplysninger om seksuelle forhold
- Andre særlige kategorier af persondata
    - Oplysninger om straffeforhold

Indhentning og videregivelse

Indhentning og videregivelse af oplysninger foregår i Forenede i henhold til gældende lovgivning.

Opbevaring samt destruktion af og adgang til persondata

Opbevaring af persondata sker i Forenede jf. gældende lovgivning på området. Dette kan betyde, at vi ikke kan slette data selvom registrerede har et ønske om dette.

Patient- og omsorgsjournaler

Patientdata skal i henhold til Journalbekendtgørelsen opbevares i minimum 10 år, og så længe der er relevant klinisk begrundelse for at opbevare dem.

Persondata på medarbejdere

Elektronisk persondata på medarbejdere opbevares i de dertil indrettede systemer, Navision og HRM. Data opbevares i 5 år efter endt ansættelse, medmindre der er en verserende sag ift. ex. en arbejdsskade.

Opbevaring af persondata, som ikke er elektroniske

Personhenførbare data, som ikke er elektroniske, opbevares i aflåste skabe, det gælder både journalmateriale og interne personalesager. Ved behov for sletning af disse data makuleres dokumenterne.

Udfasning af IT-udstyr

Ved udfasning af IT-udstyr sikres det, at personhenførbare data destrueres, således det ikke længere er muligt at læse eller genskabe data igen.

Distancearbejdspladser

Etablering af adgang fra distancearbejdspladser til Forenede kræver tilladelse fra nærmeste leder.

Der anvendes 2-faktor validering ved brug af distancearbejdsplads.

Medarbejderen er ansvarlig for sikkerheden på distancearbejdspladsen, herunder for at sikre den mod fx computervirus og hackere, såfremt der anvendes privat IT-udstyr.

Distancearbejdspladsen skal indrettes således, at eventuelle personoplysninger behandles forsvarligt og utilgængeligt for uvedkommende. Personoplysninger må ikke opbevares på distancearbejdspladsen, men alene behandles elektronisk i de centrale IT-systemer.

Ved tyveri / bortkomst af mobil / PC

Såfremt den telefon, du får tilsendt 2 faktor validering til, eller din PC bliver stjålet eller bortkommer på anden vis, så er det vigtigt du underretter IT-afdelingen snarest muligt efter det opdages, således de kan få spærret adgangen. IT vil derefter i samarbejde med direktionen beslutte om det skal politianmeldes.

Medarbejderen er ansvarlig for den fysiske sikkerhed omkring udstyret udleveret af Forenede. Det skal omgående meldes til IT, hvis udstyret bortkommer fx på grund af tyveri.

Systemer

Indkøb af systemer

Det er Forenedes IT afdeling som indkøber systemer til koncernens virksomheder. Det er således ikke tilladt at købe og installere IT systemer i Forenedes IT miljøer uden foregående, at have aftalt dette med Forenedes IT afdeling. Dette gælder også gratis software og cloud tjenester

Der henvises til dokumentet: Politik for systemanskaffelser

Anvendelse af Forenedes IT-systemer

Forenedes IT-systemer, netværk mv. skal anvendes til arbejdsrelaterede formål. Privat anvendelse af fx computere, e-mail-systemer, netværk, internettet eller telefoner skal begrænses til et minimum og må ikke påvirke den ansattes arbejdsmæssige indsats. Personlige brugerkonti og kodeord samt etableret adgang til it-systemer må ikke overdrages til andre. Brugeren er ansvarlig for eventuelt misbrug.

Al transmission af personoplysninger over internettet skal ske i krypteret form. Dette kan normalt konstateres ved at sikre sig, at der er hængelås på de websites man tilgår.

E-mail

Al kommunikation, der vedrører aktivitet i Forenede koncernen skal foregå via firma mailadresse. Denne kommunikation må ikke foregå via medarbejderes eller konsulenters private mail.

Ved afsendelse af e-mails bør emnefeltet desuden give en præcis information om e-mailens indhold, så modtageren er bekendt hermed, allerede inden e-mailen åbnes.

Det skal specielt nævnes, at privat brug af e-mail som massekommunikationsmiddel - fx i forhold til hele eller dele af Forenedes systemer, ikke er tilladt. Som eksempel herpå kan nævnes private "salgsannoncer", kædebrevsaktiviteter, "underholdningsmails" og lignende.

Er afsenderen ikke kendt, og ser indholdet mistænkeligt ud, skal meddelelsen straks slettes og It afdelingen skal have besked.

Vedhæftede filer, der indeholder videosekvenser, lyd, spil, billeder, vil blive betragtet som underholdning og accepteres ikke, medmindre indholdet har arbejdsmæssig relevans.

Er der brug for at sende en e-mail med vedhæftet fil, skal modtageren gøres tydeligt opmærksom på, hvad filen indeholder. Det er vigtigt for ikke at skabe tvivl hos modtageren om filens ægthed.

Det er ikke tilladt, at indstille fast videresending af sin mail til en ekstern mailadresse.

PC

Alle medarbejdere skal huske at låse den lokale pc, når den forlades. Dette gøres ved at trykke "CTRL+ALT+DELETE" og derefter vælge "Lås denne computer", eller Windows-L. PC'en auto-låses efter 15 minutters inaktivitet.

Forenede har installeret agenter på de lokale maskiner, som sætter os i stand til, at supportere, fjernstyre samt tage backups af dokumenter på maskinen.

Installation af software

Programmer må kun installeres efter aftale med IT-afdelingen.

Beskyttelse mod malware

I Forenede bruger vi en fysisk firewall der monitorerer al data-trafik, indgående såvel som udgående.

Herudover bruger virksomheden en spam- og virus-firewall der monitorerer al mail korrespondance, ind og ud af virksomheden.

Ydermere er alle virksomhedens PCére sikret med antivirus og DNS skanner.

Det er ikke tilladt at deaktivere eller omgå de etablerede sikkerhedsforanstaltninger.

Kommunikation

Personfølsomme oplysninger må kun sendes ud af huset, såfremt der anvendes stærk kryptering (TLS 1.2 eller højere).

Følgende gælder:

1. Elektronisk kommunikation mellem Forenede virksomheder foregår på samme system og alle e-mail sendes sikkert og krypteret
2. Elektronisk post til medarbejder i DK foregår via E-boks
3. Undtagelsesvist, hvor det ikke er muligt at sende via, E-boks, E-mail via SendSikkert eller almindeligt brev, har ledelsen i Forenede besluttet, at der kun må sendes personfølsomoplysninger eller anden følsom information til medarbejder via mail, såfremt der anvendes krypterede zip-filer og passwordbeskyttelse. Bemærk at passwordet i så fald minimum skal have en længde på 8 karakterer, og skal sendes via f.eks. sms (Bemærk, at E-boks er den foretrukne kommunikationsform til medarbejder i DK).
4. Alle som anvender en Forenede mailadresse må gerne sende personfølsomme oplysninger til andre med en Forenede mailadresse., såfremt der er en arbejdsmæssig begrundelse for dette.
5. Alle, som anvender en Forenede mailadresse må ikke sende personfølsomme oplysninger til eksterne virksomheder / samarbejdspartnere, med mindre disse virksomheder / samarbejdspartnere kan modtage en sikker mail.
6. Alle konsulenter som fra deres private eller anden eksterne arbejdsmail, ønsker at sende en e-mail med personfølsomme oplysninger til en Forenede mailadresse, skal være opmærksom på at dette ikke er tilladt.

Sikkerhedsbevidsthed

Alle har medansvar for, at Forenedes IT-systemer og data beskyttes. Medarbejdere skal løbende informeres om informationssikkerhed, således at de forskellige medarbejdergrupper kan varetage deres arbejdsopgaver på betryggende vis. Der vil med løbende blive udsendt information og læring omkring cybersikkerhed. Medarbejderen er pligtigt til læse/deltage i denne.

Dette sikres ved introduktionen af nye medarbejdere og specifikt i forbindelse med indførelse af nye systemer, processer eller retningslinjer.

Sikring af kontorer, lokaler og faciliteter

Alle kontorer hvor der forefindes IT-udstyr, indeholdende persondata eller forretningskritisk data, er aflåst når de ikke benyttes. Ved arbejdstids ophør, aflåses lokalerne altid.

Clean desk

Skriveborde skal være ryddet ved arbejdsdags ophør, således at der ikke forefindes papirer mv. indeholdende persondata på bordet.

Systemnedbrud

I tilfælde af nedbrud af kerne IT-systemer skal IT-afdelingen kontaktes straks. Der er udarbejdet handleplaner, der sikrer information, udbedring og genopretning af systemerne.

Overvågning af systemnedbrud

Alle servere overvåges 24/7/365 af hhv. Forenedes IT afdeling samt den leverandør, vi har outsourcet driften af vores servere til. Det betyder, at leverandører ved systemnedbrud hurtigst muligt sørger for, at serveren kommer op at køre igen.

Backup-procedurer

Det tages løbende backup af alle systemer hos Forenede. *Backupprocedurer fremgår af dokumentet "Backup-politik"*.

Organisation og ansvar

Den administrerende direktør i Forenede koncernen har det overordnede ansvar for informationssikkerheden.

Lederne hos Forenede har ansvar for:

- at informationssikkerhedspolitikken og de regler, der er relevante for eget ansvarsområde, er kendte og efterleves blandt egne medarbejdere
- at medarbejderne opnår sikkerhedsbevidsthed om nødvendigheden af at overholde denne informationssikkerhedspolitik, og at denne efterleves

Systemejere har ansvar for:

- sikkerhedsmæssige forhold omkring systemet, herunder at vurdere adgang og brugerrettigheder i henhold til lovgivning og interne retningslinjer.

Teknisk Afdeling / lederen lokalt har ansvar for:

- Administration af fysiske sikkerhedsforhold, herunder udlevering af nøgler og medarbejderkort og vedligeholdelse samt afprøvning af vigtige nødforsyninger som fx nødstrømsanlæg.

Alle ansatte hos Forenede er ansvarlige for:

- At efterleve informationssikkerhedspolitikken og de regler, der er relevante for den enkeltes arbejdsopgaver.

Overvågning og logning

Generelle kontrolforanstaltninger

Forende foretager logning af følgende:

- Login, mislykket login og logout på IT-systemer
- Åbning, ændring og sletning af filer på fællesdrev og personligt drev
- Åbning af hjemmesider
- Registrering af komme-/gå-tider i workforce management systemer
- Dørkontrol
- Video-overvågning på udvalgte lokationer

Mail / Outlook

IT-Afdelingen kan åbne og læse e-mails samt meddelelser i brugerens outlook, hvis det er nødvendigt af drifts- eller sikkerhedsmæssige årsager, f.eks. i forbindelse med sygdom, ferie eller fratræden, samt for at føre kontrol med medarbejderens brug af mail, samt foretage sikkerhedskopiering og genetablering. Private mails og beskeder skal mærkes "Privat" i emnefeltet og må ikke læses.

Personlige drev

Såfremt pladsforbruget op de personlige drev og onedrive øges betragteligt, forbeholder IT-afdelingen ligeledes ret til at undersøge drevene for pladskrævende filer såsom lyd og film.

Tavshedspligt

Alle ansatte skal iagttage fuldstændig tavshed omkring alle personoplysninger, som man kommer i forbindelse med i forbindelse med arbejdets udførelse hos Forenede. Der skal endvidere

Hos Forenede fremgår en medarbejders tavshedspligt og fortrolighed af medarbejderens ansættelseskontrakt. Tavshedspligten gælder også efter ophørt ansættelse.

Brud på sikkerheden

Alle brud på informationssikkerheden eller mistanke herom skal straks meddeles til IT afdelingen.

For tilknyttede personer, samarbejdspartnere og leverandører kan overtrædelse få konsekvenser i forhold til det videre samarbejde. Erstatningspådragende eller strafbare handlinger kan desuden medføre et retsligt efterspil.

Implementering

Politikken skal udleveres ved ansættelse, samt formidles til alle relevante interessenter, herunder samtlige medarbejdere med adgang til Forenedes IT systemer samt relevante underleverandører hos Forenede.

Opfølgning

Head of group IT skal mindst en gang årligt revurdere informationssikkerhedspolitikken, herunder om alle interessenter har tilstrækkeligt kendskab til politikken og afledte dokumenter.

Revurdering skal endvidere ske, hvis der foretages væsentlige ændringer i organisationen eller IT systemerne.

Personalehåndbog

Det er pr. juli 2022 besluttet, at de ansvarlige for People & Culture i Forenedes respektive selskaber spejler udvalgte dele af IT sikkerhedspolitikken i Forenedes personalehåndbøger.