CENTER FOR CYBERSIKKERHED

DIGITALISERINGSSTYRELSEN

BESKYT ORGANISATIONEN:

Opdater sikkerhedspolitikkerne til en »ny normal«

Da COVID-19 i marts måned lukkede det meste af Danmark og resten af verden ned, skulle mange organisationer med kort varsel omstille sig til at arbejde virtuelt. Distancearbejde har mange steder vist sig at være en gevinst, og mange organisationer vil sandsynligvis også "post-COVID-19" benytte sig af distancearbejde i langt højere grad end tidligere.

Men den hurtige omstilling og det øgede distancearbejde har også vist, at der nogle steder er svagheder ved denne nye arbejdspraksis. Således viser en analyse om offentligt ansattes informationssikkerhed[1], at en betydelig del af ansatte i den offentlige sektor ikke altid efterlever god sikkerhedsmæssig praksis ved distancearbejde: Lige under en fjerdedel bruger privat udstyr til hjemmearbejde, en tredjedel benytter ikke de tjenester, arbejdspladsen stiller til rådighed og mere en end tredjedel af de ansatte transporterer arbejdsrelaterede sensitive oplysninger rundt uden for arbejdet.

Derfor er der behov for, at organisationen genbesøger sine sikkerhedspolitikker[2] og retningslinjer. Dels for at sikre, at de faktisk understøtter denne måde at arbejde på og dels for at sikre, at organisationen får adresseret de særlige risici, der kan være forbundet med distancearbejde.

Samtidig skal organisationens medarbejdere være opmærksomme på, at man på baggrund af de ændrede arbejdsformer i visse tilfælde bør tilpasse sine arbejdsrutiner og adfærd. Dette adresseres i "God kultur ved distancearbejde", der indeholder en række konkrete råd målrettet den enkelte medarbejder.

[1] Digitaliseringsstyrelsen og DKCERT: Danskernes informationssikkerhed 2020
[2] Sikkerhedspolitikker dækker i denne sammenhæng politikker om informationssikkerhed, it-sikkerhed, personalesikkerhed, fysisk sikkerhed mv. I teksten vil ordene sikkerhedspolitik og politik anvendes som sideordnede begreber.

For organisationen er det vigtigt, at den ved ændringer i væsentlige forhold genbesøger relevante politikker og retningslinjer med henblik på en eventuel opdatering, således at de afspejler de aktuelle forhold og organisationens krav til sikkerhed.

Center for Cybersikkerhed og Digitaliseringsstyrelsen har udarbejdet en liste[3] med emner, der er særligt relevante at adressere i forbindelse med hjemme- eller distancearbejde. Under hvert fokusområde opstilles en række spørgsmål, som vi anbefaler, at organisationen stiller sig selv for at afklare, om gældende politikker bør opdateres. Bemærk at listen isoleret set ikke kan anvendes til udarbejdelse af en generel sikkerhedspolitik, og at de angivne eksempler ikke skal opfattes som udtømmende.

Sikkerhedspolitikker og retningslinjer

1. Hvad: Beskriver politikkerne hvordan eventuelle nye og/eller øgede risici for organisationen skal håndteres?

Hvorfor: Udbredelsen af distancearbejde ændrer organisationens risikobillede. Det anbefales, at ledelsen om nødvendig sikrer, at organisationens sikkerhedspolitikker opdateres, så de afspejler nye eller ændrede risici som følge af distancearbejde. Sker dette ikke, stiger risikoen for, at organisationen bliver ramt af uønskede hændelser.
Hvordan: Gennemgå de enkelte punkter i denne publikation og tag stilling til om de er relevante for jeres organisation. Hvis ja – indarbejd disse i jeres sikkerhedspolitikker.

Medarbejdersikkerhed

2. Hvad: Er der retningslinjer for adskillelse af privat- og arbejdsliv?

Hvorfor: Ved øget distancearbejde kan der være en tendens til, at privat- og arbejdsliv glider mere sammen. Dette kan øge risikoen for læk af interne informationer, uautoriseret adgang til interne informationer samt øget risiko for kompromittering, hvis medarbejderen eksempelvis benytter privat udstyr til arbejdsrelaterede forhold og omvendt.
Hvordan: Det anbefales, at organisationen ud fra en risikovurdering tager stilling til adskillelse mellem privat- og arbejdsliv og udarbejder de nødvendige politikker/retningslinjer. I relation til brug af privat udstyr i arbejdsmæssig sammenhæng, bør organisationen især være opmærksom på at afdækning af et udbrud af malware og den nødvendige oprydning efter et angreb, kan blive meget vanskelig og kan påføre medarbejderen tab af private data, licenser mv.
Hvis konsekvenserne ved, at medarbejderen benytter privat udstyr til arbejdsrelaterede forhold er store, bør organisationen stille det nødvendige udstyr til rådighed samt overveje at forbyde brugen af privat udstyr til arbejdsrelaterede opgaver.

[3] Listen tager udgangspunkt i mange af de overordnede emner, der er dækket af ISO 27001 standardens Annex A.

3. Hvad: Er der retningslinjer for afholdelse af virtuelle møder?

Hvorfor: Brugen af virtuelle møder kan udfordre organisationens sikkerhed, hvis en række forhold ikke er på plads. Her tænkes eksempelvis på brugen af specifikke platforme, opsætning og sikring af virtuelle møderum, godkendelse af deltagere, håndtering af præsentationsmateriale og andre dokumenter under møderne.
Hvordan: Stil godkendte, sikre og anvendelige løsninger til rådighed for medarbejderne, og beskriv hvorledes disse må/bør anvendes. Se i øvrigt CFCS publikation "Råd om sikkerhed på virtuelle mødeplatforme".

4.Hvad: Er der retningslinjer for afholdelse af arbejdsrelaterede møder uden for organisationens og hjemmets fysiske rammer, eksempelvis på caféer eller andre offentligt tilgængelige steder?

Hvorfor: En nedlukning af organisationens kontorer kan medføre, at medarbejdere bliver nødt til at mødes fysisk på anden vis for at opretholde en social kontakt eller for at tale om arbejdsrelaterede forhold. Herved øges risikoen for læk af interne informationer.
Hvordan: Præciser I jeres retningslinjer om virtuelle eller fysiske møder må afholdes i offentlige rum, og hvis ja – under hvilke forudsætninger.

Håndtering af organisationens informationer og udstyr

5. Hvad: Har organisationen klare retningslinjer for, hvordan medier og dokumenter håndteres i forbindelse med medarbejderens distancearbejde?

Hvorfor: Når en medarbejder bringer interne informationer ud af organisationen, er der en risiko for, at disse informationer ubevist falder i uvedkommendes hænder, f.eks. tab af ukrypterede USB-nøgle eller laptop.
Hvordan: Beskriv de forskellige overordnede typer af information, som organisationen råder over. For hver type af information beskriv samtidig hvilke regler/retningslinjer, der gælder for behandling af disse informationer. Eksempelvis bør organisationen beskrive, hvilke informationer, der må tages med hjem, hvordan og via hvilke medier transporten må foregå. Endelig bør organisationen beskrive hvordan informationerne skal opbevares og eventuelt bortskaffes. I den sammenhæng bør det også overvejes, om medarbejderen skal sikre, at andre personer i hjemmet ikke får adgang til informationerne.

6. Hvad: Er der retningslinjer for, hvad der kan drøftes "offentligt", og hvad der ikke kan?

Hvorfor: Når arbejdet rykker ud af organisationens kontorer og ud på offentlige steder vil der være en øget risiko for uvedkommende for indsigt i interne forhold, herunder fx personoplysninger.

Hvordan: Organisationen bør have klare regler for, hvilke interne forhold medarbejderne må drøfte offentligt. Dette bør dokumenteres i organisationens sikkerhedspolitik. Efterfølgende kan forskellige medarbejderrettede kampagner medvirke til at reglerne efterleves.

7. Hvad: Er der nedskrevne regler for udlevering og aflevering af udstyr til distancearbejde?

Hvorfor: Når arbejdspladsen rykker ud af kontoret kan medarbejderen have behov for at få noget it-udstyr hjem udover eksempelvis den bærbare pc. Organisationen bør forholde sig til, hvilket udstyr, der skal administreres, og hvordan dette skal ske. Hvis medarbejderen skal tilbagelevere udstyret til organisationen, vil det typisk fritage medarbejderen for at tage stilling til, om der er sensitive informationer eller data på udstyret, der bør slettes, inden udstyret kasseres.
Hvordan: Det anbefales, at udstyr, der udleveres til distancearbejde, registreres og som udgangspunkt håndteres på samme måde som organisationens øvrige it-udstyr for blandt andet at sikre, at det korrekte udstyr tilbageleveres, når der ikke længere er brug for det.

8. Hvad: Er der politikker/retningslinjer for medarbejderes private indkøb og brug af privat it-udstyr til brug i forbindelse med deres hjemmearbejde, herunder hvorledes dette er forsikret?

Hvorfor: I mange organisationer har medarbejderne en bærbar pc, som de kan anvende hjemmefra. Hvis arbejdssituationen kræver, at medarbejderen arbejder hjemmefra i en længere periode, vil en it-arbejdsplads kun bestående at en bærbar pc sandsynligvis ikke være tilstrækkeligt. Hvis medarbejderen oplever, at det er besværligt at få nødvendigt, supplerende udstyr fra kontoret, er det sandsynligt, at mange vil anskaffe sig udstyr uden om organisationen.
Hvordan: Det anbefales, at organisationen formulerer retningslinjer for indkøb, registrering og support af it-udstyr, såfremt arbejdspladsen ikke kan stille det til rådighed for medarbejderen.

Adgangsstyring

9. Hvad: Tages der i politikkerne særskilt stilling til, om distancearbejde kræver begrænsninger i adgangen til interne informationer eller systemer, eller om der er behov for øgede sikringstiltag?

Hvorfor: Da distancearbejde potentielt kan gøre organisationen mere sårbar, kan der være behov for at begrænse adgangen til særligt kritiske informationer. Alternativt kan der stilles specielle krav til adgangskontrollen.
Hvordan: Identificer kritiske informationer og systemer og foretag derefter en vurdering af om en kompromittering af disse (som følge af ekstern adgang) vil have alvorlige konsekvenser for organisationen. Er dette tilfældet, bør organisationen tage stilling til særlige adgangsbegrænsende og -sikrende tiltag, herunder brugen af stærkere adgangsstyring, udførlig

logning og netværksovervågning. Brugen af VPN i den sammenhæng er ligeledes et minimumskrav for statslige myndigheder.

10. Hvad: Tages der i politikkerne særligt stilling til, om - og i givet fald hvordan - brugen af privilegerede konti kan ske fra distancearbejdspladsen?

Hvorfor: Privilegerede konti er specielt attraktive for hackere. Derfor bør brugen af disse konti ske med særlig bevågenhed.
Hvordan: Hvis en medarbejder har opgaver, der kræver it-administrative rettigheder, anbefales det, at grundlaget for regler på området træffes ud fra en risikomæssig vurdering. Samtidig bør det overvejes, om brugen af de privilegerede konti kun kan ske fra specifikke pc-arbejdspladser udstyret med certifikat og kun i specifikke tidsrum.

11. Hvad: Beskriver politikkerne, om, og i givet fald hvornår, den enkelte medarbejder kan få administrative rettigheder på it-udstyr der anvendes til distancearbejde?

Hvorfor: Mange organisationer vælger at tildele hjemmearbejdende medarbejdere yderligere rettigheder for at sikre let adgang til servicefunktioner i forbindelse med installation af software mv.
Hvordan: Det anbefales, at man fastholder principperne om at begrænse medarbejders brug af privilegerede konti mest muligt og i stedet tilbyder installation af software via central software-installations-funktion eller begrænser adgang alene til en officiel app-store.

12. Hvad: Er der ændrede krav for låsning af medarbejders pc'er (pause-skærm), når de anvendes hjemme?

Hvorfor: Mange medarbejdere kan være tilbøjelige til at opfatte deres hjem som et mere sikkert sted at arbejde, hvorfor brugen af "lås-skærm-funktion" anses for overflødig.
Hvordan: Det anbefales, at politikkerne for brugen af "lås-skærm-funktion" ved distancearbejde er identisk eller skærpet i forhold til den, der gælder på kontoret.

Driftssikkerhed

13. Hvad: Er det beskrevet i politikken, hvordan den enkelte medarbejder har mulighed for at få support på udstyret derhjemme?

Hvorfor: Når medarbejderen er på kontoret vil adgangen til support ofte være "lige om hjørnet". Dette er ikke tilfældet i forbindelse med distancearbejde.
Hvordan: Det anbefales, at der udarbejdes retningslinjer for, hvordan en distancearbejdende medarbejder kan få support og eksempelvis erstatningsudstyr, hvis udstyret fejler.

14. Hvad: Beskriver politikkerne specielle handlinger, som hjemmearbejdende medarbejdere skal udføre for at sikre, at deres arbejds-pc holdes ajour i forhold til virus- og malware-beskyttelse og sikkerhedsopdateringer?

Hvorfor: Ikke alle organisationer har it-løsninger, der understøtter, at medarbejderne arbejder fuldt ud hjemmefra. Derfor kan der være risiko for, at medarbejdernes pc'er ikke modtager de nødvendige sikkerhedsopdateringer
Hvordan: Understøtter organisationens patch-management-funktion ikke fjern- eller hjemmearbejdspladser, anbefales det, at disse i stedet "falder tilbage til" den automatiske opdateringsfunktionen fra de respektive softwareleverandører.

15. Hvad: Er der i politikkerne fastsat minimumskrav til sikring af udstyr, der anvendes til distancearbejde?

Hvorfor: Når medarbejderen gør brug af distancearbejde, sker det som regel ved brug af organisationens standard-pc. Denne er normalt opsat og konfigureret med udgangspunkt i det risikobillede, der er gældende, inden for organisationens fysiske rammer. Når medarbejderen bruger pc'en uden for organisationen, er risikobilledet et andet. Der er eksempelvis en øget risiko for tyveri af enheden, når den medbringes uden for organisationen.
Hvordan: Det anbefales, at organisationen tager stilling til, om de generelle sikkerhedskrav til arbejds-pc'en bør skærpes, eksempelvis ved at sætte minimumskrav til WIFI-netværk som medarbejderen må tilgå. Et andet skærpet krav kan være, at medarbejderens pc skal anvende diskkryptering, og at udstyret slukkes, når det forlades.

16. Hvad: Er der i politikken et krav om øget overvågning af sikkerheden på medarbejdernes pc'er, når der gøres brug af distancearbejde i en længere periode?

Hvorfor: Når it-udstyr flyttes uden for organisationens fysiske rammer, vil risikoen rettet imod udstyret normalt være større. Derfor kan der ud fra en risikobetragtning være behov for øge overvågningen af disse enheder. Samtidig kan der være et behov for en løbende overvågning af, at distancearbejdspladsen er korrekt opdateret, og at installeret sikkerhedssoftware er aktivt.
Hvordan: Som udgangspunkt og under hensyntagen til eventuelle gældende regler bør medarbejderens it-udstyr til distancearbejde være underlagt den samme systemovervågning og kontrol, som it-arbejdspladsen på kontoret.

17. Hvad: Beskriver politikkerne, hvordan ændrede krav til arbejdssituationen skal håndteres i forhold til medarbejdernes behov for nye eller alternative softwareløsninger?

Hvorfor: Når medarbejderne arbejder hjemmefra, kan der opstå behov for at understøtte samarbejdet gennem brug af virtuelle samarbejdsplatforme. Stiller organisationen ikke

sådanne virtuelle arbejdsplatforme til rådighed, er der en risiko for, at medarbejderne anvender løsninger, der ikke er godkendt eller kan godkendes af organisationen.
Hvordan: Der bør etableres en proces for, hvordan nye/alternative software-løsninger kan evalueres og tages i brug inden for en tidshorisont, der tilgodeser det forretningsmæssige behov.

Sikker netværkskommunikation

18. Hvad: Er der i politikken krav om løbende overvågning af kapaciteten af VPN-forbindelsen?

Hvorfor: Når mange medarbejdere tilgår organisationens systemer hjemmefra, er belastningen af organisationens VPN-forbindelse meget høj. Hvis kapaciteten ikke er tilstrækkelig, opleves utilfredsstillende arbejdsforhold, som øger risikoen for, at medarbejderne vælger alternative og ikke-godkendte løsninger i deres arbejde.
Hvordan: Det anbefales, at kapaciteten i organisationens VPN-forbindelse og andre mulige flaskehalse løbende overvåges, og at kapaciteten om nødvendigt udvides, hvis belastningen stiger over en foruddefineret grænseværdi.

19. Hvad: Er der i politikkerne taget stilling til, om al datatrafik fra hjemmearbejdspladsen nødvendigvis skal sendes over organisationens VPN-forbindelse?

Hvorfor: Når al datatrafik fra medarbejderen sendes via VPN ind over organisationens netværk, er der en risiko for, at VPN-forbindelsen hurtigt bliver overbelastet. Dette er specielt tilfældet, hvis medarbejderne gør brug af online-møder, hvor både video og tale transmitteres via netværket. Mange VPN-løsninger understøtter en opsplitning af kommunikationen således, at eksempelvis datatrafik relateret til videomøder sendes uden om organisationens VPN løsning. Herved mindsker man risikoen for overbelastning.
Hvordan: På baggrund af en vurdering af kapacitetsbehov i forhold til kapaciteten i organisationens infrastruktur bør det overvejes (eventuelt i samråd med ens leverandør), om en opsplitning af datatrafikken fra medarbejderens distancearbejdsplads bør foretages. For ikke at forringe sikkerheden på distancearbejdspladsen bør man dog generelt følge leverandøren af VPN-løsningens anbefalinger på dette område.

20. Hvad: Er der politikker for medarbejders brug af mobiltelefoners hotspot-funktion til opkobling af medarbejder-pc'en?

Hvorfor: Risikoen for en kompromittering af medarbejderens distancearbejdsplads og organisationens systemer øges, hvis der anvendes usikre (åbne) wifi-netværk. Organisationen bør derfor medvirke til, at medarbejderne vælger en mere sikker netværksopkobling, når de arbejder væk fra kontoret.

Hvordan: Det anbefales, at organisationen gør det muligt for medarbejderen at anvende sin arbejdsmobiltelefons funktion til internetdeling (hotspot-funktion). Denne funktion skal beskyttes med kode. Bemærk at dette kan kræve ændringer i medarbejderens mobiltelefonabonnement.

21. Hvad: Dækker politikkerne aspekter vedrørende brugen af beskedtjenester i forbindelse med distancearbejde?

Hvorfor: Anvendelsen af eksempelvis ukrypterede beskedtjenester (fx. SMS) til interne/følsomme informationer kan udgøre en speciel risiko i relation til datalæk. Ifølge Datatilsynet bør følsomme personoplysninger ikke sendes via SMS.
Hvordan: Det anbefales, at organisationen på baggrund af en risikovurdering tager stilling til, hvordan og på hvilke kanaler og tjenester følsomme oplysninger kan deles.

Styring af informationssikkerhedsbrud

22. Hvad: Dækker politikkerne aspekter vedrørende håndtering af brud på sikkerheden i forbindelse med distancearbejdspladsen?

Hvorfor: Når medarbejderen i hjemmet eller i byen oplever et sikkerhedsbrud, er det vigtigt, at der er en klar forståelse af, hvad der skal gøres.
Hvordan: Det anbefales, at der etableres klare retningslinjer for et kontaktpunkt i it-afdelingen eller it-sikkerhedsfunktionen, hvis en sådan findes.

Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

23. Hvad: Er det beskrevet, hvordan organisationen sikrer at ledelse, medarbejdere og vitale funktioner kan kontaktes i en situation, hvor der arbejdes hjemmefra?

Hvorfor: Når større eller mindre dele af organisationen arbejder hjemmefra, er der behov for at sikre, at man internt i organisationen kan få fat i hinanden uafhængig af, om der er tale om en krisesituation eller blot et almindelig arbejdsrelateret aspekt.
Hvordan: Der bør fastlægges retningslinjer for ajourførte kontaktlister, der dækker, uanset om medarbejderne er på kontoret eller arbejder hjemme.

24. Hvad: Er der i politikkerne taget højde for, at ansvaret for konkrete opgaver/funktioner også skal kunne varetages, hvis større eller mindre dele af organisationen sættes i karantæne eller bliver sygemeldt?

Hvorfor: Under en pandemi eller en anden større hændelse, hvor større eller mindre dele af organisationen sættes i karantæne, vil der være behov for at sikre, at vitale funktioner i organisationen kan videreføres.
Hvordan: Det anbefales, at organisationen identificerer vitale funktioner, og at der i organisationens beredskab indarbejdes rutiner, som tager højde for, at en stor del af organisationen kan være i karantæne eller lignende.

25. Hvad: Er der nedskrevne rammer/forventninger (fx. reaktionstider) for tilkald af ledelse og/eller medarbejdere, hvis de skal møde fysisk på arbejde?

Hvorfor: Nogle bor langt fra deres arbejdsplads. Arbejder de hjemme, kan de derfor have svært ved at møde hurtigt ind, selv hvis en situationen kræver deres fysiske tilstedeværelse. Dette bør organisationen tage højde for i krise- og beredskabsplaner og om nødvendigt sikre alternative supportmuligheder.
Hvordan: Der bør udarbejdes en kontaktliste, hvor eksempelvis medarbejderens forventede rejsetid til kontoret fremgår. For hver medarbejder bør der udpeges en suppleant med kortere transporttid, der om nødvendig kan inddrages. Eventuelt under supervision af den primære medarbejder.

26. Hvad: Er der i politikkerne for nød- og beredskabssituationer taget højde for aspekter vedrørende begrænsning af tilstedeværelsen af medarbejdere i samme rum?

Hvorfor: Det kan være umuligt at samle mange personer i forbindelse med en krisestyringssituation.
Hvordan: Organisationen bør tænke i muligheder for at organisere krisestyringen på en måde, så hele krisestaben ikke behøver at være samlet ét sted.

27. Hvad: Indgår hjemmearbejdspladser i organisationens politikker for styring af nød- og beredskabssituationer, og hvordan sikres i givet fald deres adgang til organisationens infrastruktur i disse situationer?

Hvorfor: Organisationens beredskabsplan bør ikke være begrænset af kun at kunne fungere, hvis alle relevante medarbejdere er fysisk tilstede i organisationen. Man bør derfor fastlægge, hvilke opgaver og funktioner, der eventuelt kan håndteres udenfor organisationens fysiske rammer.
Hvordan: For hver opgave, der er beskrevet i beredskabsplanen bør der tages stilling til om denne opgave kan udføres via en distancearbejdsplads.

28. Hvad: Er situationer knyttet til distancearbejde omfattet af organisationens test af beredskabsplaner?

Hvorfor: Det er vigtigt, at rutiner, mødesteder, roller og anvendte kommunikationskanaler er grundigt afprøvet, inden en eventuel krise rammer, uafhængigt af om organisationen i øvrigt gør brug af distancearbejde.
Hvordan: Indarbejd brugen af distancearbejdsplads i organisationens test af beredskabsplaner.

Overensstemmelse

29. Hvad: Hvordan sikres det, at ledelse og medarbejdere kender og følger relevante sikkerhedspolitikker i forbindelse med distancearbejde?

Hvorfor: Information om og styring af organisationens sikkerhedsmæssige setup er typisk mere besværligt ved medarbejdernes distancearbejde.
Hvordan: Det anbefales, at organisationen i sin sikkerhedsstyring tager højde for distancearbejdende medarbejdere, således at relevant opfølgning og kontrol også fungerer efter hensigten under disse forhold.

30. Hvad: Beskriver politikkerne, hvordan der kan føres tilsyn med it-sikkerheden i forbindelse med distancearbejde?

Hvorfor: Afhængig af den enkelte organisation kan der være et større eller mindre behov for at føre tilsyn med, at de sikkerhedsmæssige forhold på medarbejdernes it-arbejdsplads overholdes.
Hvordan: Sikkerhedspolitikkerne skal klart fastlægge og synliggøre rammer og forventninger til tilsyn med it-sikkerheden på hjemmearbejdspladsen.

31. Hvad: Beskriver politikkerne, hvordan nødløsninger og mindre formelle it-sikkerhedsrelaterede dispensationer skal gennemgås og håndteres på lidt længere sigt?

Hvorfor: Mange organisationer er i forbindelse med den aktuelle pandemi gået på kompromis med deres egne sikkerhedspolitikker. Dispensationer bør aldrig vare evigt. Organisationen bør forholde sig til den ændrede situation, hvis den får længere varighed.
Hvordan: Det anbefales, at der fastlægges regler for, hvor længe eksisterende dispensationer kan accepteres, før der skal foretages tilretninger af de oprindelige regler og retningslinjer

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

DIGITALISERINGSSTYRELSEN

Postboks 2193
1017 København K
Telefon: 3392 5200
E-mail: digst@digst.dk