Djøfs it-politik

Revideret april 2023

Djøf

Indholdsfortegnelse

1. HUSKELISTE TIL DIT DAGLIGE ARBEJDE 4

1.1 Huskeliste 4
1.1.1 Generel sikkerhed 4
1.1.2 Persondatasikkerhed 4

1.2 Mistanke om sikkerhedsbrud mv 5
1.3 Opmærksomhedspunkter 5

2. INDLEDNING 6

3. PERSONER OMFATTET AF DISSE RETNINGSLINJER 7

4. GENERELLE RETNINGSLINJER FOR ANVENDELSE AF INFORMATIONSTEKNOLOGI 8

4.1 Retningslinjer for brug af internettet 8
4.2 Retningslinjer for brug af mail 8
4.3 Retningslinjer for brug af SMS til medlemmer, ikke-medlemmer og øvrige samarbejdsparter 8
4.4 Retningslinjer for brug af medarbejdersignaturer 8

5. HVAD HAR DJØF ADGANG TIL? 9

5.1 Adgang til mails 9
5.2 Adgang til telefoner 9
5.3 It-sikkerhed og logning 9

6. RETNINGSLINJER FOR BRUG AF CLOUD-SERVICES OG UDVEKSLING AF INFORMATIONER VIA CLOUD- OG FILDELINGSTJENESTER 10

6.1 Brug af cloudtjenester – godkendte som fx Zoom og Microsoft365 10

7. GENEREL SIKKERHED I FORBINDELSE MED IT 12

7.1 Sikkerhed i forbindelse med it-udstyr 12
7.1.1 Når det personlige udstyr er ude af syne 12
7.1.2 Når du arbejder udenfor Djøf 12

7.2 Sikkerhed i forbindelse med anvendelse af pc-programmer, it-tjenester samt ønske om nye programmer/it-tjenester mv. 13
7.3 Sikkerhed i forbindelse med mobiltelefon/iPads 14
7.4 Sikkerhed i forbindelse med USB-stik og andre bærbare datamedier 14

8. SIKKERHED I FORBINDELSE MED LOGIN OG PASSWORDS 15

8.1 Regler for passwords 15

9. FYSISK SIKKERHED I KONTORER 16

9.1 Kontorer 16
9.2 Netværksstik 16
9.3 Helpdesk 16

10. MISTANKE OM ELLER KONSTATERING AF CYBER- ELLER VIRUSANGREB 17

11. MISTANKE OM ELLER KONSTATERING AF PERSONDATABRUD 18

12. OVERHOLDELSE AF DISSE RETNINGSLINJER 19

1. Huskeliste til dit daglige arbejde

Du skal altid overholde Djøfs it-politik, og denne huskeliste hjælper dig til at følge reglerne i dit daglige arbejde. Du kan printe huskelisten ud og have den ved din computer, så du hurtigt kan tjekke, såfremt der er noget, du bliver i tvivl om sikkerhedsmæssigt i forhold til håndtering af data og dine enheder samt anvendelsen af disse.

1.1 Huskeliste

1.1.1 Generel sikkerhed

> Du må aldrig videregive dine personlige passwords til andre.

> Du skal altid aktivere din låseskærm, når du forlader din pc (Windows-tasten og et L).

> Du skal altid udvise forsigtighed, inden du klikker på links samt downloader filer og være opmærksom på, at mails kan være sendt af it-kriminelle.

> Du må ikke tilgå hjemmesider med indhold eller downloade indhold, der er ulovligt i henhold til dansk lovgivning, og det er strengt forbudt at benytte it-systemerne til på nogen måde at udføre eller deltage i ulovlige aktiviteter.

> Du må udelukkende modtage og anvende USB-stik, du har fået fra en samarbejdspartner, hvor det er aftalt med denne, at materialet leveres via et USB-stik. Finder du et USB-stik, må det IKKE anvendes, men skal afleveres til IT.

> Du må aldrig viderestille din Djøf-mail til en mailkonto uden for Djøf.

> Du må ikke tilknytte private pc'ere til Intunes

> Du skal hurtigst muligt opdatere din iOS/Android enhed, når nye versioner frigives, medmindre du får anden besked fra IT. Dette kommunikeres også anledningsvist på Djøfs intranet.

> Du må kun downloade apps, der sendes ud fra Apple App Store og fra Android Google Play Store eller mobilproducentens egen Store.

> Gæster, der skal bruge eget udstyr på nettet, skal tilslutte sig Gæstenetværket djoef-guest.

> Der må kun tilsluttes godkendt Djøf-udleveret udstyr til Djøfs netværk.

> Du skal altid lukke din pc HELT ned, inden den transporteres eller opbevares udenfor Djøf.

> Du skal lukke din pc HELT ned, inden du går hjem for at sikre at opdateringer kommer på. Hvis du ikke lukker din pc helt ned regelmæssigt, modtager du en mail med påmindelse om at gøre det. Efterlades den i Djøf ved arbejdstidens ophør, skal den gemmes et ikke synligt sted.

1.1.2 Persondatasikkerhed

Personoplysninger er oplysninger, som på enhver tænkelig måde kan henføres til en bestemt person. Fx kontaktoplysninger, et medlemsnummer, et portrætbillede, en ip-adresse mv.

- Du må kun opbevare absolut nødvendigt materiale med personoplysninger i fysisk form. Hvis du finder dokumenter med personoplysninger et uautoriseret sted, skal du fjerne dem og give dem til den ansvarlige Djøf-medarbejder eller makulere dem.

- Materiale med personoplysninger må ikke smides i skraldespanden, men skal smides i de bokse med låg, der er placeret i printerrummene. Herfra makuleres materialet.

- Vælg dine mailmodtagere med omtanke, og sæt kun cc-personer på, hvis det er relevant.

- Hvis du skal sende personoplysninger eksternt

  - i forbindelse med en ny arbejdsgang, som fx til en ny samarbejdspartner
  - som enkeltstående masseudsendelse – (ved mange modtagere og altid ved flere end 100 modtagere)
  - hvis du skal vedhæfte dataudtræk

  skal du kontakte din chef, inden du sender oplysningerne. Vær opmærksom på, at masseudsendelser kun må foretages af særligt udpegede medarbejdere i MKP og DA.

- Du må kun gemme personoplysninger i Microsoft365, MR4, HR-systemer og andre systemer, der er GDPR compliant. I særlige tilfælde kan det tillades at gemme personoplysninger på et netværksdrev. IT har udrullet struktur for netværksdrev, hvor netværksdrev oprettes efter formål. Indhold slettes automatisk efter besluttede regler. Spørg i IT, såfremt du er i tvivl.

- Du må ikke gemme personoplysninger på dit skrivebord (c-drev), USB-stik, hukommelseskort i telefoner eller i andre usikre systemer, fx Dropbox.

- Du må aldrig sende personoplysninger i SMS-tekster.

1.2 Mistanke om sikkerhedsbrud mv

- Hvis du har mistanke om et it-sikkerhedsbrud (som fx at du er blevet hacket, har fået virus eller andet), skal du straks fjerne alle stik fra din computer og få denne slukket (hold powerknappen nede til den slukker). Kontakt straks derefter IT, og orienter derefter din chef.

- Ved mistanke om brud på persondatasikkerheden (som hvis du fx har sendt persondata til forkert modtager), skal du stoppe hændelsen og kontakte din chef. Hvis din chef ikke er tilgængelig på dagen, skal du kontakte en af Djøfs andre chefer. Indrapporter herefter databruddet via TOPdesk. Se punkt 11. Mistanke om eller konstatering af persondatabrud

1.3 Opmærksomhedspunkter

- Du skal altid indhente godkendelse fra din chef samt MDA Governanceudvalget (via behovsskabelon sendt til DataOgAnalyseEnhed@djoef.dk), inden du tager nye pc-programmer eller it-tjenester i brug. Det gælder også gratis programmer og tjenester.

2. Indledning

Anvendelsen af informationsteknologi i Djøf er uundværlig og med til at forbedre og effektivisere Djøfs services og administrative funktioner.

Djøf betragter derfor medarbejdernes kendskab til og fortrolighed med it som vigtig.

Brug af it, internettet og mail betyder dog også, at vi alle må forholde os til en lang række risici og muligheder for bevidst eller ubevidst misbrug.

Som følge heraf er det vigtigt, at du anvender it, internettet, mails, systemer og services med samme grad af omhu, omtanke, forsigtighed og anstændighed, som du i øvrigt udviser i det daglige arbejde, og at du kun tilgår oplysninger, som du har et arbejdsbetinget behov for.

I Djøf skal alle medarbejdere gennemføre og bestå e-læringskurser i it-sikkerhed og GDPR. E-læringskurserne er obligatoriske, og alle medarbejdere skal årligt re-certificeres.

Alle medarbejdere og andre med adgang til Djøf, herunder Djøfs systemer, er underlagt tavshedspligt.

3. Personer omfattet af disse retningslinjer

Disse retningslinjer er gældende for alle, der

> har fået udleveret personligt udstyr (som fx pc) eller en telefon af Djøf.
> har fået adgang til systemer, services eller data hos Djøf.

Alle personer, der er omfattet af denne it-politik, og som er ansat i Djøf eller arbejder med systemer og services, er forpligtet til at holde sig ajour med de heri beskrevne retningslinjer og vil årligt blive bedt om at bekræfte at have læst it-politikken.

Som omfattet af denne it-politik er du ligeledes forpligtet til at holde dig ajour på Djøfs intranet, hvor der løbende kommunikeres nyt vedrørende it-sikkerhed.

4. Generelle retningslinjer for anvendelse af informationsteknologi

4.1 Retningslinjer for brug af internettet

Det er ikke tilladt at tilgå hjemmesider med indhold eller downloade indhold, der er ulovligt i henhold til dansk lovgivning. Herunder gælder også download af ophavsrettighedsbeskyttet indhold, som fx musik og film. Djøf tillader sig at blokere for hjemmesider, der ikke er arbejdsrelaterede og samtidig kan udgøre en sikkerhedsrisiko.

Internetadgangen må endvidere ikke anvendes til at formidle informationer eller materiale, der kan virke stødende, uetisk eller moralsk forkasteligt i relation til race, religion, nationalitet, politisk eller seksuel overbevisning mv.

4.2 Retningslinjer for brug af mail

Se Djøfs mail-vejledning på Djøfs intranet.

4.3 Retningslinjer for brug af SMS til medlemmer, ikke-medlemmer og øvrige samarbejdsparter

Der må ikke fremgå personoplysninger eller fortrolige oplysninger i en SMS.

4.4 Retningslinjer for brug af medarbejdersignaturer

Har du brug for en medarbejdersignatur skal dette godkendes af din chef. Se Medarbejdersignatur-vejledning på Djøfs intranet under "vejledninger".

Du skal være opmærksom på, at de oplysninger du kan se i systemerne der kræver medarbejdersignatur er fortrolige og ikke må deles med andre.

5. Hvad har Djøf adgang til?

5.1 Adgang til mails

Djøf betragter dine mails og vedhæftede filer som Djøfs ejendom, både mails i Outlook og MR4 Sag og Djøf har derfor adgang til dine mails ved fravær og af andre drifts- og sikkerhedsmæssige årsager.

Hvis en mail fremtræder som privat, må indholdet ikke læses. Hvis det ved åbning af en mail viser sig, at den er privat, skal den straks lukkes igen.

Du skal, hvis det er muligt, varskos inden Djøf tilgår mails medmindre der er tale om mistanke om strafbare forhold eller forhold, der kan få ansættelsesretlige konsekvenser.

Du skal altid orienteres efterfølgende, såfremt det har været nødvendigt at læse dine mails.

5.2 Adgang til telefoner

IT kan IKKE læse dine SMS beskeder/messages, mails, se billeder eller andet privat på din iPhone/iPad.

IT kan kun se, de apps du får installeret fra Djøf på din mobiltelefon/tablet. Derudover kan IT se oplysninger om enhedens model, software version og telefonnr. mm.

IT og de i afdelingerne der er administratorer, kan i 3Kontakt se, hvilke telefonnumre du har ringet op samt modtaget opkald fra. Ligeledes kan tidspunkt samt varighed for opkaldene ses.

5.3 It-sikkerhed og logning

Af hensyn til bl.a. pålidelig drift, sikkerhed, genetablering og dokumentation opbevares alle mails i Office365, hvorfra indholdet sikkerhedskopieres dagligt.

IT logger alt trafik på internettet fra alle pc'er og kan på ethvert tidspunkt se, hvilke hjemmesider der er tilgået fra ovennævnte pc'er. Ligeledes logges de apps, du åbner, og hvilke lokationer du er på, når du anvender din Office365 konto.

I MR4 Basis logges dine ændringer og i F2 (Sag) logges både dine opslag (læsning) og dine ændringer i sagen med dine medarbejderinitialer og tidspunkt. Logningerne gemmes i separate filer, som kun Data og Analyse har adgang til. Data og Analyse har mulighed for at foretage løbende stikprøver i logfilerne.

Alle mails sendt til og fra Djøf i Outlook logges af IT med afsender, modtager og emne.

Al trafik ind og ud af Djøf bliver logget i firewall´en.

Alle FollowMe-printere i Gothersgade logger, hvad der bliver printet af hvilke medarbejdere.

Ved mistanke om uregelmæssigheder eller overtrædelser af interne regler kan loginoplysningerne bruges til at kortlægge medarbejdernes brug af internettet og interne systemer.

6. Retningslinjer for brug af cloud-services og udveksling af informationer via cloud- og fildelingstjenester

6.1 Brug af cloudtjenester – godkendte som fx Zoom og Microsoft365

Det er vigtigt, at du udelukkende anvender de cloudtjenester som Djøf har indgået en kontrakt og en databehandleraftale med. Dette gør det tilladt at anvende dem til konkrete arbejdsprocesser og data. Det er fx Zoom og Microsoft365.

Retningslinjer for anvendelsesformål for Zoom vs. Teams:

- Zoom Meetings eller Webinars benyttes til medlemsrettede online arrangementer.
- I de tilfælde hvor en medlemsrettet aktivitet ikke kan afvikles i Zoom benyttes Teams Meetings. Tilmeldingsflow må håndholdes manuelt. Spørg evt. juridisk afdeling til råds.
- Til almindelig mødeaktivitet kan benyttes det værktøj Zoom/Teams, man finder mest anvendeligt til formålet.

For nærmere vejledning om brug af Zoom anbefales det at se i Zoom-vejledningen på Djøfs intranet under 'vejledninger/møder/zoom videomøde'.

Retningslinjer for anvendelsesformål for transport af data, der pga. størrelsen ikke kan deles på anden vis:

- Her skal afdelingens Ekstern Deling Sites anvendes.

Alle øvrige cloudtjenester bør du betragte som et 'offentligt sted', hvor alle har adgang. Derfor er det afgørende, at du ikke videregiver/lægger oplysninger i disse clouds, som ikke tåler offentliggørelse. Det er derfor ikke tilladt at formidle/lægge materiale i clouds, der indeholder personoplysninger af nogen art, eller på anden vis er fortroligt.

Herunder er nogle eksempler på, hvad du må lægge op, og hvad du ikke må lægge op i clouds uden godkendt anvendelsesformål:

- Det er tilladt at lægge materiale op vedr. et arrangement, men ikke deltagerlisten da denne indeholder navne.
- Det er tilladt at lægge billeder og videoer op, men ikke, hvis der er billeder eller lyd, der kan bruges til at identificere medlemmer eller andre personer.
- Det er ikke tilladt at sende dokumenter til medlemmer i clouds uden godkendt anvendelsesformål, som indeholder personoplysninger eller oplysninger vedr. kontakt med Djøf, som fx ansættelseskontrakter.
- Det er ikke tilladt at lægge personhenførbare informationer fx fra MR4 i clouds uden godkendt anvendelsesformål, dette gælder også udtræk eller lignende.
- Det er ikke tilladt at lægge brugernavn og koder til Djøfs systemer i clouds uden godkendte anvendelsesformål.
- Det er ikke tilladt at lægge forretningskritisk/hemmelig information i clouds uden godkendte anvendelsesformål.

Ovenstående er især vigtigt, hvis du deltager i et webinar eller et onlinemøde i fx Teams, som er arrangeret af en ekstern person. Husk altid, at være varsom med at klikke på links i mails, du får

tilsendt uopfordret. Det kan lukke virus ind i virksomhedens it-systemer. Du kan kontrollere, hvor et link peger hen ved at holde musemarkøren over.

Hvis du er i tvivl, skal du kontakte din chef, inden du anvender en løsning i clouds uden godkendte anvendelsesformål

7. Generel sikkerhed i forbindelse med it

7.1 Sikkerhed i forbindelse med it-udstyr

It-udstyret indkøbes af IT og ejes af Djøf. Du kan ikke selv vælge udstyr. IT tager hensyn til dit ergonomiske behov i samarbejde med Djøfs tilknyttede ergoterapeut. It-udstyret skal opbevares forsvarligt, og skal behandles med omhu.

7.1.1 Når det personlige udstyr er ude af syne

Personligt udstyr er mest udsat for tyveri og misbrug, når det ikke er under opsyn.

Efterlades din pc i Djøf ved arbejdstidens ophør, skal du gemme den et ikke synligt sted, fx i en skuffe eller i et skab.

Under transport og opbevaring udenfor Djøf, skal din pc til enhver tid være lukket ned i en sådan tilstand, at der kræves hardware system password (det første password der indtastes, inden du logger på systemerne).

Mister du din pc, skal du hurtigst muligt ringe til IT på 3395 9950, da dette er akut. Kan du ikke få kontakt til IT oprettes en TOPdesk sag. IT vil så spærre alle it-adgange, så snart det er muligt. Alle filer, der udelukkende er gemt på pc'en, går tabt, hvis pc'en mistes eller går i stykker.

Du skal så vidt muligt undgå at opbevare private filer/dokumenter på din Djøf-pc. Kan dette ikke undgås, kan du oprette en mappe på dit OneDrive og navngive den 'Privat'. Såfremt du gemmer på dit c-drev skal du huske at der ikke tages backup af data på c-drevet, og at det, der opbevares der, forsvinder såfremt pc'en går i stykker, stjæles, reinstalleres eller rammes af virus.

Ved planlagt fravær ud over ferie, fx barsels- og forældreorlov af under tre måneders varighed, kan du efter aftale med din chef tage din bærbare pc med hjem. Det kræver en aftale, fordi alle Djøfs pc'er automatisk bliver sikkerhedsopdateret, når de er på Djøfs net. Det sker enten ved, at pc'en fysisk anvendes i Djøf eller ved at koble pc'en op til internettet med vpn-forbindelsen til Djøf. Det er muligt at gå på nettet uden anvendelse af vpn, og jo længere tid der går uden en vpn-opkobling med Djøf, desto større risiko er der for, at pc'en bliver inficeret med virus og/eller malware og derfra spreder sig til hele Djøfs it-system. Du skal derfor mindst hver 14. dag logge på med vpn og have pc'en tændt svarende til en arbejdsdag, så pc'en kan blive opdateret.

Ved planlagt fravær af over 3 måneders varighed skal pc'en afleveres til IT.

Afleverer du din pc, kan du ikke forvente at få den samme pc tilbage efter orlov. Derfor er det vigtigt, at du ikke har dokumenter, programmer eller andet liggende lokalt på pc'en (fx skrivebord, c-drev).

Hvis du har en mobiltelefon/iPad (du kan evt. låne en iPad i Djøf i orlovsperioden), kan du installere Firmaportal og via vpn få forbindelse til Djøfs intranet og følge med i det sociale liv i Djøf.

7.1.2 Når du arbejder udenfor Djøf

Nedenstående gælder for såvel hjemmearbejde, som når du i øvrigt arbejder udenfor Djøf.

Djøfs pc'er, tablets og mobiltelefoner er udstyret med en krypteret VPN-forbindelse, og derfor må du gerne tilslutte din pc mv. til en wi-fi-forbindelse uden for Djøf, fx fra et hotel, en cafe mv.

Herunder er nogle gode råd ved hjemmearbejde og øvrigt arbejde udenfor Djøf:

- Brug Microsoft365 platformen og MR4
  Benyt kun de godkendte systemer – altså Microsoft365, MR4 og godkendte fildrev - der er fx backup og den generelle sikkerhed på plads. Hvis du bliver nødt til at gemme dokumenter med personoplysninger lokalt på computeren, skal du huske at flytte dem over i Microsoft365/MR4 (eller til rette fildrev) så snart det kan lade sig gøre og derefter slette den lokale kopi.
- Du må som udgangspunkt ikke tage fortrolige oplysninger eller personoplysninger på papir med ud af Djøf. Hvis det er nødvendigt at have oplysningerne med på papir, fx til et møde uden for huset, skal du sørge for at have oplysningerne ved dig hele tiden. Når der ikke er brug for at have oplysningerne på papir længere, skal de makuleres. Hvis der er behov for at gemme oplysningerne, skal de skannes ind i Microsoft365/MR4.
- Print kun det nødvendige, og smid det ikke i skraldespanden.
  Print kun papirer med personoplysninger, hvis det er nødvendigt. Har du papirer med oplysninger om fysiske personer, så sørg for både at opbevare og skaffe dem af vejen på betryggende vis. Du kan fx gemme dem i en skuffe og tage dem med ind i Djøf, når du er tilbage, så de kan blive makuleret. Du må ikke smide dem i din egen skraldespand.
- Tal altid i enrum, hvis det er personfølsomt.
  Vær opmærksom på ikke at dele personoplysninger, når du fører fortrolige telefonsamtaler uden for Djøf, hvis der er andre i samme rum. Du kan fx gå ind i et rum, hvor du kan tale alene, eller du kan undlade at sige navnet og andre oplysninger, der kan identificere det medlem, du taler med.
- Lås skærmen.
  Husk at låse skærmen på din computer, når du forlader den og vær opmærksom på, at andre så vidt muligt ikke bør kunne se skærmen, når du arbejder. Rekvirer eventuelt et skærmfilter til din pc. Dette kan bestilles via TOPdesk. Når du ikke arbejder på din pc, så sørg for at lukke den helt ned. På den måde er Djøfs data bedre beskyttet i tilfælde af indbrud eller tyveri.
- Undlad at åbne og læse private mails fra dine private mailkonti på din arbejdscomputer. Det skyldes, at disse ikke har den samme beskyttelse som Djøfs mails, og derved udsætter du Djøfs systemer for en risiko, når du åbner dine private mails på pc'en. Brug hellere din telefon eller iPad til at læse private mails og mailkonti.

7.2 Sikkerhed i forbindelse med anvendelse af pc-programmer, it-tjenester samt ønske om nye programmer/it-tjenester mv.

Såfremt du i dit arbejde ønsker eller har behov for at anvende

- et relevant program, der ligger uden for de af IT installerede standardprogrammer
- en betalt it-tjeneste, for eksempel leveret af en ekstern leverandør
- en gratis it-tjeneste, for eksempel en gratisapp

skal det godkendes af din egen chef samt MDA-Governanceudvalget, inden programmet eller tjenesten tages i brug.

MDA Governanceudvalget har til formål at sikre imødekommelse af Djøfs behov for systemunderstøttelse og it-tjenester under hensyntagen til it-sikkerhed, it-arkitektur, persondatabeskyttelse/lovgivning og økonomi. Behov beskrives (gennem udfyldelse af behovsskabelon) og godkendes af egen chef forud for fremsendelse til udvalgssekretariatet (DataOgAnalyseEnhed@djoef.dk.). Behovet fremlægges i MDA Governanceudvalget. MDA Governanceudvalget i Djøf har repræsentanter fra Direktion, DIT, DA og JUR.

Det er vigtigt, at du kontakter din chef i god tid, da der ofte vil skulle indgås aftaler med udbyder/leverandør, inden programmet eller tjenesten kan tages i brug. Dette gælder særligt, hvis anvendelsen af programmet eller tjenesten indebærer behandling af personoplysninger.

Såfremt en ekstern konsulent skal tilknyttes længerevarende i Djøf, hvor adgang til de nødvendige systemer via djoef-guest ikke er tilstrækkelig, rettes der henvendelse til HR, der har udarbejdet en politik for adgang til Djøfs netværk. Herudover kontaktes IT.

7.3 Sikkerhed i forbindelse med mobiltelefon/iPads

Mobiltelefonen/iPads skal sikres med kode eller biometrisk som fingeraftryk m.v..

Hvis du ønsker adgang til din Djøf-mail, kalender, MR4 Sag, MR4 Basis eller Djøfs intranet fra din mobiltelefon/iPad, skal du installere Firmaportal på enheden. Data på iOS modeller, der anvendes i Djøf, er krypterede. Du skal sørge for, hurtigst muligt (medmindre du får anden besked fra IT) at opdatere din iOS/Android enhed når nye iOS/ Android versioner udsendes. Ligeledes skal du opdatere apps, når nye versioner frigives. Dette kommunikeres også anledningsvist på Djøfs intranet.

Du må kun downloade apps der sendes ud fra Apple App Store, Androids Google Play Store eller mobilproducentens egen Store. Ved download af apps fra andre steder, er der stor risiko for at inficere din telefon/iPad med programmer, der kompromitterer dens stabilitet og sikkerhed. Ovenstående 'Stores' er producenternes egne kanaler til apps, og yder en vis form for sikkerhed, da de har gennemlæst kildekoden, før de har publiceret deres apps. Det er forbudt, at 'jailbreake' eller 'roote' - dvs. at fjerne spærringen producenten har lagt på din telefon/iPad.

Hvis du mister en Djøf mobiltelefon eller iPad, skal du straks henvende dig til 3's telefoniske selvbetjening på 70 313 123 for at få spærret dit simkort samt til IT for at få slettet indholdet på enheden.

7.4 Sikkerhed i forbindelse med USB-stik og andre bærbare datamedier

Finder du et USB-stik på Djøfs lokaliteter, skal du aflevere det til IT.

Personoplysninger må kun gemmes i Microsoft365, MR4 og andre særligt indrettede systemer, aldrig lokalt på pc, USB eller lignende. Der skal udvises stor påpasselighed med filer, der overføres til USB eller andre bærbare datamedier. Ellers er der risiko for, at filer kan offentliggøres, hvis et bærbart datamedie mistes.

Du må udelukkende modtage og anvende USB-stik, du har fået fra en samarbejdspartner, hvor det er aftalt med denne, at materialet leveres via et USB-stik. Dette kunne fx være fra en anerkendt organisation eller virksomhed.

Hvis du er i tvivl, om du kan gemme personoplysninger på et system uden for Microsoft365 eller MR4, skal du kontakte din chef.

8. Sikkerhed i forbindelse med login og passwords

8.1 Regler for passwords

Dit password udløber hver 3. måned. Du modtager en mail om dette i god tid. Dit password:

> skal være på minimum 15 tegn og kan indeholde både små og store bogstaver samt tal og tegn
> må ikke indeholde æ, ø eller å
> må ikke indeholde dit navn eller dine initialer
> må ikke indeholde 4 ens tegn efter hinanden
> må ikke være det samme som et af dine 10 sidste passwords

Du vil af sikkerhedsmæssige årsager blive låst ude af Djøfs systemer efter 6 forkerte indtastninger af dit password. Kontakt IT, hvis du bliver låst, så de kan låse op for dig.

Du må ikke bruge dit Djøf-password andre steder end til dit Djøf-login. Har du password til andre Djøf-relaterede eksterne systemer, fx gennem Djøfs samarbejdspartnere, må du ikke genbruge dit Djøf-password. Lav i stedet et nyt og stærkt password (fx minimum 10 karakterer, store/små bogstaver, tal og tegn).

Dit password er privat og du må aldrig videregive dine personlige passwords til andre. Skriv aldrig passwords ned på papir. Opbevar dem sikkert i fx e-boks.

9. Fysisk sikkerhed i kontorer

9.1 Kontorer

Der er i Djøf almindelig adgang til kontorerne inden for normal arbejdstid.

Følgende indgange til Djøf er videoovervåget:

> Indgangene ved Gothersgade
> Receptionsområdet
> Mellemgang fra Gothersgade til gården
> AC's indgang ved Nørre Voldgade
> Ved udgangene til gårdområderne

Uden for normal arbejdstid er der kun adgang til bygningerne for medarbejderne ved hjælp af en nøglebrik, kode eller nøgle.

Medarbejderen skal sikre, at eventuelle fortrolige Djøf-udskrifter og andet materiale, der indeholder personoplysninger og øvrige oplysninger, som er eller må sidestilles med forretningshemmeligheder, opbevares på en måde, så de ikke kan misbruges. Materialet må ikke smides i skraldespanden, men skal smides i de opstillede bokse i printerrummene. Ligeledes er der mulighed for makulering hos Teknisk Service.

9.2 Netværksstik

Der må kun tilsluttes godkendt Djøf-udleveret udstyr til netværksstik i Djøf.

9.3 Helpdesk

Alle medarbejdere i Djøf har adgang til Djøfs helpdesk system TOPdesk. Du finder link til TOPdesk på Djøfs intranet.

10. Mistanke om eller konstatering af cyber- eller virusangreb

Det er vigtigt, at du straks tager kontakt til IT ved mistanke om virus eller sikkerhedsbrud, som fx hvis:

> du har mistanke om, at en mail indeholder links, der kan være skadelige.
> du modtager opkald fra 'fremmede' der vil have adgang til din pc.
> din computer eller dine programmer pludselig opfører sig 'mærkeligt', fx kører meget langsomt, sender usædvanlige skærmmeddelelser eller data ser underlige ud.
> gæster forsøger at tilslutte sig vores eget interne netværk via kabel – gæster skal henvises til gæstenetværket (djoef-guest).

Klik aldrig på links eller åbn vedhæftninger, hvis du er i tvivl om, hvorvidt det er en spam/virusmail. Hvis du modtager en mail i din indbakke, hvor du er i tvivl om, hvorvidt det er en spam/virusmail, skal du sende mailen videre til IT ved at anvende SPAM-knappen i Outlook.

Er du kommet til at klikke på et link eller åbne en vedhæftning i en spam/virusmail, skal du straks fjerne alle stik fra din computer og få denne slukket (hold powerknappen nede til den slukker). Derefter skal du øjeblikkeligt og vedvarende forsøge at komme i kontakt med IT og orientere din chef.

Når du har kontakt med IT, vil de på baggrund af en kort problemanalyse udstikke en række anvisninger, som du er forpligtet til at følge. Vær opmærksom på at et virusangreb kan udgøre et brud på persondatasikkerheden. Se afsnit 11.

Du må hellere kontakte IT en gang for meget end en gang for lidt ved mistanke om virus eller sikkerhedsbrud.

11. Mistanke om eller konstatering af persondatabrud

Da det er lovpligtigt at behandle, dokumentere og risikovurdere ethvert databrud der inkluderer persondata, skal alle databrud indrapporteres internt i henhold til proceduren for rapportering af brud på persondatasikkerhed (se vejledning på Djøfs intranet under "vejledninger" – "GDPR i Djøf"), uanset hvilken afdeling de sker i, hvem der foretager eller konstaterer dem, deres type/format og deres risikoniveau.

Eksempler på databrud

I Djøf vil databrud typisk opstå i form af:

> E-mails fremsendt til/filer delt med forkert modtager
> Mistet enhed (mobiltelefon/PC)
> Medlems-stamdata fejlregistreret/slettet
> Medlemsoplysninger videregivet uden hjemmel
> Fejl i/mangelfuld adgangsstyring i IT-systemer resulterende i uautoriseret adgang til oplysninger.

Håndtering og rapportering af databrud

Hvis du har mistanke om, konstaterer, eller af anden vej informeres om et databrud, skal du:

> hvis det er muligt, herefter stoppe bruddet f.eks. ved at trække forkerte sendte e-mails tilbage (om muligt), korrigere evt. fejl indlæsninger, stoppe job kørsler mv.
> orientere din chef. Hvis din chef ikke er tilgængelig på dagen, skal du kontakte en af Djøfs andre chefer.

Herefter skal du indrapportere databruddet via TOPdesk:

> Vælg "TOPdesk" i højre sidemenu på forsiden af Djøfs intranet.
> Vælg "Databrudsrapportering" fra TOPdesk-menuen.
> Udfyld (alle) formularens felter og tryk "indsend".
> Du modtager nu en bekræftelsesmail fra TOPdesk, med en databrudsrapport-skabelon vedhæftet i Word-format.
> Åben Word-dokumentet og udfyld databrudsrapport-skabelonens (kun del 1) så fyldestgørende som muligt. Skabelonen indeholder hjælpetekster og eksempler, som vejleder dig i udfyldelsen.
> Gem den udfyldte databrudsrapport lokalt og returnér herefter dokumentet til DPO-organisationen hurtigst muligt ved at besvare bekræftelsesmailen fra TOPdesk og vedhæft dokumentet.
> DPO-organisationen modtager din databrudsrapport, og tager herefter direkte kontakt til dig med eventuelle spørgsmål, generel opfølgning på din rapportering og omkring den efterfølgende håndtering af bruddet.

Der gælder korte tidsfrister for eventuel indberetning til Datatilsynet og underretning af de berørte personer, og det er derfor vigtigt, at sagen i TOPdesk oprettes inden for 6 timer.

Al kommunikation med medier, Datatilsynet, offentlige myndigheder mv. sker i overensstemmelse med Djøfs politik for kommunikation ved it-nedbrud, hackerangreb mv. For evt. rapportering til Datatilsynet sker dette altid via DPO-organisationen. Hvor det er relevant at notificere berørte personer, sker dette via forretningen i tæt koordination med DPO-organisationen.

12. Overholdelse af disse retningslinjer

I denne it-politik er beskrevet en række regler og retningslinjer for sikker, etisk og forretningsmæssig fornuftig brug af it. Det er vigtigt at forstå, at brud på disse retningslinjer kan forstyrre driften og skade Djøf, vores medlemmer og involvere myndighederne. Overtrædelse af reglerne betragtes derfor med stor alvor.

Det er Djøfs politik at vise medarbejderne tillid og åbenhed, og dette gælder naturligvis også i forhold til brugen af it, mail og internettet. Som medarbejder i Djøf har vi alle i vores daglige arbejde et medansvar for vores medlemmers og kollegaers sikkerhed. Det ansvar forventes alle at leve op til ved brugen af it og håndteringen af data.

I tråd med politikken om åbenhed, tillid og troværdighed er det strengt forbudt at benytte it-systemerne til på nogen måde at udføre eller deltage i ulovlige aktiviteter. Konstateres sådanne aktiviteter, kan det føre til politianmeldelse og /eller anmeldelse til anden relevant myndighed. Brug af Djøfs it-udstyr, der er i strid med disse retningslinjer, og som potentielt kan skade Djøfs sikkerhed og omdømme, kan i særlig grove tilfælde få konsekvenser for ansættelsesforholdet og eventuelt medføre krav om erstatning.