Frederiksberg Kommunes It-sikkerhedsregler (baseret på ISO 27001)

December 2019

Indhold

Regler

1. Informationssikkerhedspolitikker

1.1 Retningslinjer for styring af informationssikkerhed

1.1.1 Politikker for informationssikkerhed

- Direktionen er ansvarlig for at godkende Frederiksberg Kommunes informationssikkerhedspolitik og It-sikkerhedsregler en gang årligt.
- Projektleder for databeskyttelse sikrer at kommunens informationssikkerhedspolitik og It-sikkerhedsregler kommunikeres ud til alle medarbejdere via intranettet.
- Projektleder for databeskyttelse sikrer at informationssikkerhedspolitikken og It-sikkerhedsreglerne er kommunikeret til samarbejdspartnere samt øvrige personer, der er involveret i anvendelsen af data og informationer i Frederiksberg kommune.
- Al information i elektronisk form som er væsentlig for kommunens varetagelse af opgaver, skal lagres i kommunens centrale it-systemer.

1.1.2 Gennemgang af politikker for informationssikkerhed

- Projektleder for databeskyttelse er ansvarlig for at informere direktionen om ændringer, der gør den gældende informationssikkerhedspolitik utilstrækkelig.
- Projektleder for databeskyttelse er ansvarlig for at revidere kommunens informationssikkerhedspolitik og It-sikkerhedsregler en gang årligt og sende dem til høring i organisationen.

1.1.3 Termer og definitioner

- Adgangsstyring: middel til at sikre, at adgang til ”aktiver” er autoriseret og begrænset på grundlag af forretnings- og sikkerhedsmæssige krav
- Aktiv: alt der har værdi for Frederiksberg kommune
- Data: Enhver form for information.
- Dataansvarlig: Chef eller leder, der alene eller sammen med andre afgør, til hvilke formål og med med hvilke hjælpemidler der må foretagers behandling af oplysninger.
- Databehandler: Den fysiske person eller den leverandør, der behandler oplysninger på den dataansvarliges vegne.
- Fortrolighed: egenskaben, at information ikke gøres tilgængelig eller kan afsløres for uautoriserede personer, entiteter eller processer
- Informationssikkerhed: bevarelse af fortrolighed, integritet og tilgængelighed af information.
- Systemejer: Den chef/leder som har kompetence til at træffe beslutning om hvordan en it-system skal anvendes.
- It-systemer: Det eller de tekniske løsninger, der behandler eller gennem Informationer / Data
- Sikkerhedsbrud: Er en fuld sikkerhedshændelse, der ikke kan håndteres og afhjælpes uden at kommunens sikkerhed er blevet kompromiteret med eventuel efterfølgende skadevirkning.

- Sikkerhedshændelse er starten på et sikkerhedsbrud, men som stadig kan håndteres og eventuelt afværges uden store konsekvenser for kommunen.
- Sikkerhedssvaghed: Er, når der er faretegn for en potentiel sikkerhedshændelse eller endog sikkerhedsbrud, men som kan lukkes ved afhjælpende foranstaltninger, inden det opstår.
- Tilgængelighed: egenskaben at være tilgængelig og anvendelig fra en autoriseret entitet.

2. Organisering af informationssikkerhed

2.1 Intern organisering

2.1.1 Funktionsadskillelse

- Arbejdsgange i it-driften skal ved funktionsadskillelse tilrettelægges så risikoen for bevidst eller ubevidst misbrug af privilegier til it-systemer minimeres
- Såfremt det ikke er muligt at indføre funktionsadskillelse i praksis, skal der etableres kompenserende kontrolforanstaltninger.

2.1.2 Kontakt med myndigheder

- Databeskyttelsesrådgiveren er i samarbejde med Projektleder for databeskyttelse ansvarlig for kontakt til offentlige myndigheder vedrørende emner inden for informationssikkerhed.

2.1.3 Kontakt med særlige interessegrupper (Bruger grupper, tværkommunale erfa grupper o.a.)

- Projektleder for databeskyttelse er ansvarlig for at der fra kommunens side opretholdes kontakt til interessegrupper eller fora inden for informationssikkerheds området.

2.1.4 Informationssikkerhed ved projektstyring

- Digitaliserings-projektledere skal sikre, at informationssikkerhed bliver en indarbejdet del af alle projekter igennem samarbejde med projektleder for databeskyttelse.

2.2 Mobilt udstyr og fjernarbejdspladser

2.2.1 Mobilt udstyr

- Fortrolig information herunder fortrolige personoplysninger, må ikke lagres lokalt på bærbare pc'er, mobiltelefoner/smartphones, tablets og andet mobil it-udstyr.
- Ved særlige behov er det tilladt at lagre fortrolig information på mobilt it-udstyr, såfremt informationerne beskyttes med adgangskode og en krypteringsløsning, som er godkendt af It-afdelingen. It-afdelingen skal vedligeholde en liste over godkendte løsninger.

2.2.2 Fjernarbejdspladser

- Privat it-udstyr må ikke anvendes til løsning af arbejdsopgaver, hvor der indgår fortrolig information herunder personoplysninger.

3. Personalesikkerhed

3.1 Før ansættelsen

3.1.1 Ansættelsesvilkår

- Projektleder for databeskyttelse sikrer at der ved ansættelsen er forpligtigelse til gennemlæsning og accept af medarbejderens ansvar i relation til informationssikkerhed i kommunen.

3.1.2 Ansættelsesbetingelser

- Projektleder for databeskyttelse sikrer at der til stadighed findes opdaterede informationssikkerhedsregler.

- Medarbejderen kvitterer ved ansættelsen for at have læst og forstået kommunens Informationssikkerhedspolitik og It-sikkerhedsreglerne. Dette sker gennem Tjekliste for grundviden om databeskyttelse og informationssikkerhed.

3.2 Under ansættelsen

3.2.1 Ledelsesansvar

- Direktion og afdelingschefer samt øvrige ledere sikrer, at medarbejderne vedvarende informeres og motiveres til at være opmærksomme på og overholde kommunens informationssikkerhedspolitik, sikkerhedstiltag og procedurer.

3.2.2 Bevidsthed om uddannelse og træning i informationssikkerhed

- Medarbejdere skal ved ansættelsen henvises til relevant informationsmateriale om sikkerhed på intranettet.
- Projektleder for databeskyttelse er ansvarlig for at medarbejderne vedvarende uddannes i og informeres om kommunens informationssikkerhedspolitik, sikkerhedstiltag og procedurer.

3.3 Ansættelsesforholdets ophør eller ændring

3.3.1 Ansættelsesforholdets ophør eller ændring

- Ved fratrædelse skal medarbejdere orienteres om, ansvar efter ansættelsens ophør, herunder tavshedspligt og andre forpligtelser. (Se også 4.1.3)
- Afdelingscheferne er ansvarlige for at informere it-afdelingen, når ansatte eller eksternt personale tilknyttet kommunen fratræder.

4. Styring af aktiver (It-systemer og andre informationsbærende kilder)

4.1 Ansvar for aktiver

4.1.1 Fortegnelse over aktiver

- It-afdelingen sørger for, at der føres en ajourført oversigt over alle anvendte it-systemer og informationsbærende kilder.

4.1.2 Ejerskab af aktiver

- Der skal udpeges en systemejer i organisationen for hvert aktiv i form af alle it-systemer og informationsbærende kilder.
- It-afdelingen sørger for, at der føres en ajourført oversigt over systemejerskabet for alle væsentlige anvendte it-systemer og informationsbærende kilder.

4.1.3 Tilbagelevering af aktiver

- Ved fratrædelse skal medarbejdere tilbagelevere alt udleveret it-udstyr, som tilhører kommunen, herunder pc'er, mobiltelefoner med videre. (Se også 3.3.1)
- Hvert område fastlægger en procedure for returnering af udleveret informationsudstyr til afdelingen i forbindelse med fratrædelse af ansat, eller anden form for personale tilknyttet kommunen.

4.2 Klassifikation af information

4.2.1 Klassifikation af information

- Projektleder for databeskyttelse fastlægger en procedure rettet mod medarbejderne, for klassificering af data og informationer i henhold til fortrolighed, personfølsomhed, personoplysninger og almindelige data.

4.3 Mediehåndtering

4.3.1 Styring af bærbare medier

- Flytbare lagrings medier, som for eksempel USB-nøgle, cd, dvd og lignende, må ikke anvendes til lagring af fortrolige informationer, med mindre der anvendes en krypterings løsning, som er godkendt af It-afdelingen og Projektleder for databeskyttelse.
- Datamedier, samt papir, som indeholder fortrolig information, skal opbevares aflåst i perioder, hvor informationen ikke anvendes.

4.3.2 Bortskaffelse af medier

- Kasserede datamedier (harddiske, cd-medier, flash-hukommelse, mv.) skal slettes eller destrueres i henhold til It-afdelingens procedurer for sletning og kassation af datamedier.
- Kasseret papir med fortrolige oplysninger eller information, som kan misbruges, skal opbevares i beskyttede beholdere og skal bortskaffes ved makulering.

5. Adgangsstyring

5.1 Forretningsmæssige krav til adgangsstyring

5.1.1 Politik for adgangsstyring

- Politik for adgangsstyring skal fastlægges, dokumenteres og gennemgås på grundlag af forretnings –og Informationssikkerhedskrav.
- Der fastlægges en procedure rettet mod afdelingschefer og bemyndigede for tildeling af adgangsrettigheder.

5.1.2 Adgang til netværk og netværkstjenester

- Brugerne skal kun have adgang til de netværk og netværkstjenester, som de specifikt har behov for, for at kunne løse deres opgaver.

5.2 Administration af brugeradgang

5.2.1 Brugerregistrering og afmelding

- Enhver form for brugeradgang til it-systemer skal ske via personlige og individuelle bruger-id.
- Brugeridentiteten bruges til at spore medarbejdernes aktiviteter på de enkelte systemer. Brugeren er ansvarlig for aktiviteter, udført under brugerens brugeridentitet.
- Fælles brugerkonti må ikke anvendes til it-systemer.
- Projektleder for databeskyttelse kan kun give dispensation til brug af fælles brugerkonti i meget sjældne tilfælde, hvor behovet kan dokumenteres.
- Fælles brugerkonti må under ingen omstændigheder benyttes i forbindelse med adgang til it-systemer, hvor der er adgang til fortrolige personoplysninger.

5.2.2 Tildeling af brugeradgang

- Tildeling, ændring og nedlæggelse af brugerautorisationer til it-systemer skal ske via kommunens formelle procedure for brugerstyring. Som udgangspunkt må man kun autoriseres til at behandle data, som er nødvendig for at løse sine arbejdsopgaver.
- Undtagelser fra anvendelsen af den formelle procedure i forbindelse med brugerautorisationer må udelukkende ske i samråd med projektleder for databeskyttelse. Ændringer skal dokumenteres.

5.2.3 Styring af privilegerede adgangsrettigheder

- Udvidede adgangsrettigheder (administratorrettigheder) til systemer, skal begrænses til personer med arbejdsbetingede behov.

- Udvidede adgangsrettigheder skal være knyttet til særlige individuelle bruger-id. Anvendelsen af rettighederne skal begrænses til opgaver og områder, hvor det er teknisk påkrævet.

5.2.4 Styring af hemmelig autentifikationsinformation om brugere

- Leverandørers standard-adgangskoder til indkøbt it-udstyr/systemer skal ændres til fortrolige adgangskoder før idriftsættelse af udstyret/systemet.
- Alle adgangskoder er fortrolige og må ikke kunne ses i klartekst ved log on på udstyret/systemet.

5.2.5 Gennemgang af brugeradgangsrettigheder

- Der skal mindst en gang hvert halve åt foretages opfølgning på brugerautorisationer, som giver adgang til fortrolige personoplysninger i it-systemer. For øvrige systemer en gang årligt
- Opfølgninger på brugerautorisationer skal dokumenteres.
- Lederen af afdelingen er ansvarlig for at sikre, at opfølgningerne udføres.
- Der skal mindst en gang årligt foretages opfølgning på udvidede adgangsrettigheder (administratoradgang) til it-systemer. For it-systemer, som behandler fortrolige personoplysninger dog mindst en gang hvert halve år. Opfølgningen skal dokumenteres.

5.2.6 Inddragelse eller justering af adgangsrettigheder

- Ved ændringer i arbejdsopgaver og organisatoriske tilknytning skal der ske opfølgning og korrekt tilpasning af den enkelte medarbejders brugerautorisationer.
- Den enkelte medarbejderens adgangsrettigheder til kommunens it-systemer og fysiske lokaliteter skal inddrages fra det tidspunkt medarbejderen fratræder sin stilling.
- I tilfælde af bortvisning/afskedigelse/fritstilling af en medarbejder skal alle medarbejderens adgangsrettigheder til it-systemer og fysiske lokaliteter inddrages omgående.

5.3 Brugernes ansvar

5.3.1 Brug af hemmelig autentifikationsinformation

- Personlige adgangskoder skal som minimum bestå af 8 karakterer og indeholde både store og små bogstaver samt tegn eller tal, de skal udskiftes mindst hver 3. måned, og de må ikke genbruges.
- Adgangskoder til brugerkonti med administrator rettigheder skal som minimum være 10 karakterer lange og indeholde både store og små bogstaver samt tegn eller tal, de skal udskiftes mindst hver 3. måned, og de må ikke genbruges.
- Personlige adgangskoder til kommunens it-systemer skal behandles fortroligt og må aldrig afsløres over for andre.
- Personlige adgangskoder til kommunens it-systemer må ikke nedskrives på papir eller lagres elektronisk uden passende beskyttelse.
- Personlige adgangskoder skal omgående ændres, hvis andre har fået kendskab til dem, eller hvis der er mistanke om dette.
- Ekstern adgang til kommunens interne it-systemer skal beskyttes gennem anvendelse af to-faktor autentifikation.
- Det er ikke tilladt at anvende samme adgangskoder, som benyttes på eventuelle private konti eller på privat udstyr.

5.4 Styring af system- og applikationsadgange

5.4.1 Brug af privilegerede systemprogrammer

- Systemværktøjer må kun anvendes af medarbejdere med påkrævede drifts- og supporttekniske opgaver i forbindelse med it-systemer.
- Systemværktøjer som kan omgå sikringsforanstaltninger må kun være aktive, når de konkret benyttes til eksempelvis fejlfinding i systemer.

6. Fysisk sikring og miljøsikring

6.1 Sikre områder

6.1.1 Fysisk perimetersikring

- Server rum og lignende sikrede områder, hvor der opbevares kritisk informationsbehandlingsudstyr, skal holdes aflåst og beskyttes med passende adgangskontrol- og alarmsystem.

6.1.2 Fysisk adgangskontrol

- Kun medarbejdere med rutinemæssige arbejdsopgaver må autoriseres med permanent adgang til server rum og lignende sikrede områder.

6.1.3 Beskyttelse mod eksterne og miljømæssige trusler

- Særligt brandbare materialer, herunder papir, pap og lignende må ikke opbevares i server rum og andre lignende sikrede områder.
- Server rum skal være beskyttet med automatisk brandslukningsanlæg og brandalarm.
- Serverrum og centrale netværkskomponenter skal være forsynet med nødstrøm, som tillader kontrolleret nedlukning i tilfælde af forsyningssvigt.
- Mad og drikke må ikke fortæres i server rum og lignende sikrede områder.

6.1.4 Arbejde i sikre områder

- Ikke-autoriserede personer, herunder eksterne serviceleverandører, skal ledsages til, under ophold og fra sikre områder af en autoriseret person
- Der skal føres logbog over ikke-autoriserede personers adgang til sikrede områder.

6.2 Udstyr

6.2.1 Placering og beskyttelse af udstyr

- It-udstyr som er kritisk for kommunens virksomhed og/eller indeholder fortrolig information skal opbevares i sikrede områder. It-beredskabsplanen (niveau II plan) skal indeholde oversigt over sikre områder.
- Server rum og lignende sikrede områder må udelukkende benyttes til opbevaring af relevant udstyr og materiale.
- Information om sikrede områder, herunder indretning og formål skal opbevares fortroligt, og informationen må kun være tilgængelig for medarbejdere med funktionsmæssige behov (it-afdelingen og relevante personer i Beredskabet..

6.2.2 Understøttende forsyninger (forsyningssikkerhed)

- Elforsyningen til centralt it-udstyr, herunder servere og netværksudstyr, skal være beskyttet mod strømafbrydelser via nødstrømsanlæg (UPS).
- Nødstrømsanlæg, skal være implementeret sådan, at tilsluttede servere automatisk kan nedlukkes korrekt og sikkert i tilfælde at strømafbrydelser.

6.2.3 Sikring af kabler

- Kabler og udstyr i serverrum, krydsfelter og andre centrale installationer, skal mærkes klart og entydigt.
- Centralt netværksudstyr, herunder krydsfelter, skal være placeret i aflåste rum eller skabe.

6.2.4 Vedligeholdelse af udstyr

- It-udstyr skal vedligeholdes og repareres efter leverandørens forskrifter
- Service og reparationer af it-udstyr må kun udføres af leverandører, som har indgået formelle serviceaftaler med kommunen.
- Der skal foretages særlig registrering af it-udstyr, som fjernes fra kommunens lokaliteter af eksterne parter, f.eks. ved reparation af udstyr. Den eksterne part skal kvittere for modtagelse af udstyret.

6.2.5 Sikring af udstyr og aktiver uden for organisationen

- Bærbare pc'er, mobiltelefoner, datamedier og andet mobilt it-udstyr, må ikke efterlades uden overvågning på offentligt tilgængelige steder.
- It-afdelingen fastlægger procedure for, hvorledes bærbart udstyr må anvendes.

6.2.6 Sikker bortskaffelse eller genbrug af udstyr

- It-udstyr som kasseres eller på anden måde afhændes, skal sikres mod, at lagrede data efterfølgende kan genskabes. Indbyggede lagringsmedier skal slettes eller destrueres i henhold til It-afdelingens procedure for sletning og kassation af datamedier.

6.2.7 Brugerudstyr uden opsyn

- Alle pc-arbejdspladser og mobile enheder, skal fra centralt hold være forsynet med skærmlås, som aktiveres automatisk efter 15 minutter
- Undtagelser: følgende udstyr er undtaget fra kravet om automatisk skærmlås:
    - Tansplejens PCer i de kliniklokaler, hvor selve tandbehandlingen sker.
    - Bibliotekernes selvbetjenings PCer til håndtering af udlån.
    - Borgerservice PCer til brug for kommunens borgere
    - PCer i vagtcentralen.
- Den enkelte medarbejder skal manuelt aktivere skærmlåsen (genvejstast ”Win+L”) eller aflåse lokalet, når en pc efterlades.
- Pc-skærme i betjeningsområder skal placeres således at fortrolige oplysninger ikke er synlige for uvedkommende.
- Printer og faxmaskiner, som benyttes til udskrift og modtagelse af fortrolig information skal placeres utilgængeligt for publikum. Alternativt skal fortrolig-udskriftsfunktion på printere benyttes.

7. Driftsikkerhed

7.1 Driftsprocedurer og ansvarsområder

7.1.1 Dokumenterede driftsprocedurer

- Tekniske installationer skal være dokumenterede. Dokumentationen skal ajourføres straks ved enhver gennemført ændring.
- Diagnose og konfigurationsporte i netværksudstyr må kun være aktive i tidsrum, hvor det er påkrævet som følge af drifts- og vedligeholdelsesmæssige opgaver.

7.1.2 Ændringsstyring

- Enhver ændring i it-driftsmiljøet skal udføres i henhold til fastlagte processer for ændringsstyring.
- I særlige situationer, hvor der opstår behov for afvigelse fra ændringsstyringsprocesserne, skal it-chefen og projektleder for databeskyttelse orienteres inden ændringen gennemføres.
- Ændringer i standard-it-systemer skal begrænses mest muligt. Der må kun foretages ændringer, som er nødvendige for driften, eller som forbedrer sikkerheden.

7.1.3 Kapacitetsstyring

- Der skal foretages løbende overvågning af ressourceforbrug og kapacitet i it-infrastrukturen, med henblik på at opretholde driftsikkerheden i forretningskritiske it-systemer.

- Med udgangspunkt i den løbende overvågning, skal der foretages regelmæssige vurderinger og fremskrivninger af behovet for udvidelser i kapaciteten. It-afdelingen skal sikre, at vurderingen gennemføres mindst en gang årligt. Resultatet skal dokumenteres i en skriftlig rapport.

7.1.4 Adskillelse af udviklings-, test- og driftsmiljøer

- Udviklings-, test- og driftsmiljø skal være adskilte for at nedsætte risikoen for uautoriseret adgang til eller ændringer af driftsmiljøet.
- It-afdelingen fastlægger en godkendelsesprocedure for overgang fra testmiljø til driftsmiljø.

7.2 Beskyttelse mod malware (Skadevoldende programmer og kode)

7.2.1 Kontroller mod malware

- Enhver server og klient-pc på kommunens interne netværk skal være forsynet med sikringsforanstaltninger som beskytter mod skadevoldende programmer og kode.
- Mobiltelefoner, smartphones/tablets og andet mobilt it-udstyr, som kan tilsluttes kommunens netværk, skal være forsynet med sikringsforanstaltninger som beskytter udstyret mod skadevoldende programmer og kode.
- Sikringsforanstaltninger til beskyttelse mod skadevoldende programmer og kode, skal holdes opdateret via automatiserede rutiner og så ofte det teknisk er muligt.
- Alt e-post - ud og indgående - skal skannes centralt og renses for skadevoldende programmer og kode.
- Al datatrafik mellem kommunens administrative netværk og internettet skal overvåges af centrale værktøjer, som kan fjerne eller blokere mod skadevoldende programmer og kode og andre typer datatrafik, som udgør en sikkerhedsrisiko for kommunens interne it-systemer.
- Servere og pc-arbejdspladser skal i videst mulig omfang konfigureres med henblik på at modstå skadevoldende programmer og kode, samt forsøg på hacking.
- Unødvendige services og funktionalitet på servere og pc-arbejdspladser skal deaktiveres for at undgå sårbarheder og muligheder for misbrug.

7.3 Backup

7.3.1 backup af information

- Al elektronisk information, som har betydning for kommunens varetagelse af opgaver, skal sikkerhedskopieres fra centralt hold.
- Kritiske it-systemer i driftsmiljøet skal løbende sikkerhedskopieres fra centralt hold.
- Sikkerhedskopiering skal ske via automatiserede rutiner.
- Der skal foretages regelmæssig afprøvning af om sikkerhedskopieret data kan gendannes i praksis.
- Datamedier med sikkerhedskopier, skal beskyttes mod uautoriseret adgang og fysiske skader som følge af brand og lignende.
- Sikkerhedskopier af kritiske data skal løbende overføres til og opbevares på en lokalitet, som er geografisk adskilt fra driftslokaliteten.
- Der skal etableres en procedure, som sikrer at Backup ikke opbevares længere end lovgivningen for forskellige datatyper tillader.

7.4 Logning og overvågning

7.4.1 Overvågning af systemanvendelse (Hændelseslogning)

- Der skal foretages en grundig vurdering af behovet for overvågning/logning i forbindelse med det enkelte it-system. Det besluttede logningsniveau skal beskrives i systemdokumentationen.
- Medarbejdernes anvendelsen af brugerkonti og autorisationer til kommunens it-systemer skal logges.
- It-systemer som anvendes til behandling og lagring af følsomme personoplysninger, skal være indrettet med logningsfaciliteter, som lever op til logningskravene i databeskyttelsesforordningen.
- Logoplysninger om anvendelse af personoplysninger skal opbevares i seks måneder og skal herefter slettes. Ved særlige behov kan logoplysningerne undtagelsesvis gemmes i op til fem år.

- Behovet for bevaring og sletning af logoplysninger i forbindelse med øvrige it-systemer skal fastlægges og dokumenteres for det enkelte it-system.
- Fejl i kritiske it-systemer skal logges maskinelt. Der skal dagligt foretages gennemgang og opfølgning på disse fejllogs.

7.4.2 Beskyttelse af log-oplysninger

- Logoplysninger fra it-systemer skal beskyttes mod manipulation og tekniske fejl, eksempelvis ved hjælp af sikkerhedskopiering, adgangsbegrænsning og konsolidering af logoplysninger.

7.4.3 Administrator – og operatørlog

- Aktiviteter som udføres i it-systemer af systemadministratorer og andre med udvidede rettigheder skal logges maskinelt.

7.4.4 Tidssynkronisering

- Ure i kritiske it-systemer, herunder server- og netværksudstyr, skal automatisk synkroniseres med præcis tidsangivelses. Tidssynkroniseringen skal regelmæssigt kontrolleres og korrigeres.

7.5 Styring af driftsoftware

7.5.1 Softwareinstallation på driftsystemer

- Styresystemer og andet software på pc-arbejdspladser og servere, skal via fastlagte arbejdsrutiner holdes forsvarligt opdateret mod kendte fejl og sårbarheder, som kan udgøre en sikkerhedsrisiko.
- Systemdokumentation skal være fortroligt og adgangen til systemdokumentationen skal begrænses til medarbejdere med fagligt begrundede behov.
- Systemdokumentation skal beskyttes med kryptering, hvis det sendes til eksterne parter via internettet eller andre åbne netværk.

7.6 Sårbarhedsstyring

7.6.1 Styring af tekniske sårbarheder

- Eksternt tilgængelige it-systemer, som kommunen selv varetager driften af, skal regelmæssigt og som minimum én gang årligt, testes for mulige sårbarheder. Testen skal iværksættes af It-afdelingen.
- Med udgangspunkt i det aktuelle trusselsbillede skal der regelmæssigt foretages vurderinger af om kommunens it infratruktur er tilstrækkeligt beskyttet mod relevante trusler.
- Vurderingen skal foretages mindst én gang årlig, eller ved større ændringer i it-infrastrukturen.

7.6.2 Begrænsninger på softwareinstallation

- Medarbejdere må ikke installere programmer og andet software på pc-arbejdspladser uden forudgående godkendelse fra It-afdelingen.
- It-afdelingen kan implementere tekniske spærringer mod installation af specifikt software på pc'er, tablets, smartphones og lignende, hvis softwaren vurderes at medføre væsentlige og unødige sikkerhedsrisici for kommunen

7.7 Overvejelser i forbindelse med revision af informationssystemer

7.7.1 Kontroller i forbindelse med revision af informationssystemer

- Projektleder for databeskyttelse er ansvarlig for at it-revisionen er aftalt med de relevante personer inden den udføres, og skal foregå på en sådan måde, at den forstyrrer den daglige drift mindst muligt.

8. Kommunikationssikkerhed

8.1 Styring af netværkssikkerhed

8.1.1 Netværksstyring

- It-udstyr må kun tilsluttes kommunens netværk efter godkendelse fra It-afdelingen.
- Der må kun anvendes netværksudstyr (herunder trådløst netværksudstyr), der er godkendt og stilles til rådighed af It-afdelingen.
- Gæster og eksterne konsulenters it-udstyr, skal gennemgå en sikkerhedskontrol og godkendes hvis udstyret skal have adgang til kommunens administrative netværk.

8.1.2 Opdeling af netværk

- It-systemer, som af driftstekniske årsager ikke kan underlægges de centralt styrede sikkerhedspolitikker skal isoleres fysisk eller logisk fra andre systemer på kommunens netværk.

8.2 Informationsoverførsel

8.2.1 Politikker og procedurer for informationsoverførsel

- Projektleder for databeskyttelse fastlægger en procedure for beskyttelse af data ved informationsudveksling imellem it-systemer.

8.2.2 Aftaler om informationsoverførsel

- Systemejeren sikrer, at der underskrives en databehandlingsaftale omhandlende omfang, ansvar, kontrol, erstatning, ejerskab og identifikation inden informationsudveksling til andre eksterne it-systemer. (Se også 10.1.2)

8.2.3 Elektroniske meddelelser

- Fortrolig information og personfølsomme data, som sendes digitalt til eksterne modtagere skal beskyttes med kryptering. Dette gøres ved forsendelse til digital post eller ved brug af sikker mail.

8.2.4 Fortroligheds – og hemmeligholdelsesaftaler

- Alle medarbejdere i kommunen får ved ansættelsen udleveret en erklæring til gennemlæsning om fortrolighed i ansættelsen efter straffelovens § 152 og forvaltningslovens § 27.
- Alt eksternt personale, der i deres arbejde skal have adgang til kommunens netværk, underskriver en aftale om ekstern samarbejdspartners adgang til it-systemer. (Se også 3.1.1)

9. Anskaffelse, udvikling og vedligeholdelse af systemer

9.1 Sikkerhedskrav til informationssystemer

9.1.1 Analyse og specifikation af informationssikkerhedskrav

- Ved udvikling og anskaffelse af nye it-systemer skal der, så tidligt som muligt og før idriftsættelse, gennemføres en grundig vurdering af de sikkerhedsmæssige aspekter. It-afdelingen og databeskyttelsesrådgiveren skal inddrages i vurderingen. (Se vedtagne retningslinjer i SLA på InSite):
  http://intra.frederiksberg.dk/Vaerktoejer/it-web-telefoni/digitaliseringsogbyggeprojekter/Sider/Digitaliseringsprojekter.aspx

9.1.2 Sikring af applikationstjenester på offentlige netværk

- Såfremt services og tjenester som udbydes på internettet af tredjepart, ønskes anvendt i forbindelse med kommunens informationsbehandling, kan dette udelukkende ske efter tilladelse fra it-afdelingen.

9.2 Sikkerhed i udviklings- og hjælpeprocesser

9.2.1 Sikker udviklingspolitik

- Anskaffelser og installation af nyt it-udstyr og software, skal ske via It-afdelingens service desk.
- It-afdelingen skal sikre, at der foretages en sikkerhedsmæssig vurdering og godkendelse af nyt it-udstyr og software, inden anskaffelsen.

9.2.2 Principper for udvikling af sikre systemer

- Installation af nye it-systemer i driftsmiljøet, skal ske i henhold til en fastlagt proces for installation af nye it-systemer.
- I særlige situationer, hvor det kan være nødvendigt at afvige fra den vedtagne proces, skal projektleder for databeskyttelse godkende, inden installationen igangsættes.
- Overførsel af it-systemer fra test- til driftsmiljø skal ske i overensstemmelse med en fastlagt procedure for idriftsættelse af it-systemer.

9.3 Testdata

9.3.1 Sikring af testdata

- Produktionsdata som indeholder fortrolig information eller personoplysninger må ikke anvendes til test og undervisningsformål.
- Såfremt tungvejende forhold nødvendiggør det, kan produktionsdata med fortrolig information og personoplysninger dog undtagelsesvis anvendes i test-sammenhæng.
- Projektleder for databeskyttelse skal godkende anvendelsen af fortrolig produktionsdata til testformål.
- Hvis fortrolig information eller personoplysninger efter godkendelse anvendes i testmiljø, skal der benyttes adgangs- og kontrolforanstaltninger efter samme krav som gælder for driftsmiljøet.

10. Leverandørforhold

10.1 Informationssikkerhed i leverandørforhold

10.1.1 Informationssikkerhedspolitik for leverandørforhold

- Ved indgåelse af aftaler med eksterne parter, skal der foretages vurderinger af alle relevante sikkerhedsmæssige risici og aspekter ved aftalen.
- Såfremt det er behov for at give eksterne parter adgang til kommunens it-systemer og information, skal der foretages en vurdering af de sikkerhedsmæssige forhold, og en tro- og loveerklæring skal underskrives inden adgangen gives.
  (Se også 8.2.4)

10.1.2 Håndtering af sikkerhed i leverandøraftaler

- Samarbejdsaftaler med eksterne samarbejdspartnere som vedrører kommunens informationsbehandlingssystemer, skal omfatte instrukser til leverandøren om alle relevante sikkerhedsmæssige aspekter udfærdiget i en databehandlingsaftale.
- Frederiksberg Kommune anvender KOMBIT's databehandlerskabelon eller alternativt Datatilsynets skabelon.
- Systemejer er ansvarlig for at eksterne leverandører oplyses om relevante ændringer i informationssikkerhedsreglerne
-

10.2 Styring af leverandørydelser

10.2.1 Overvågning og gennemgang af leverandørydelser

- Der skal foretages regelmæssig opfølgning på de sikkerhedsmæssige aspekter ved de aftaler, som er indgået med eksterne samarbejdspartnere.

- Systemejerne skal sikre, at der minimum en gang årligt sker opfølgning på sikkerheden ved aftaler med eksterne samarbejdspartnere, herunder sikre, at revisorerklæringer medtages og vurderes.

10.2.2 Styring af ændringer af leverandørydelser

- Systemejeren er ansvarlig for at der ved ændringer i formelle samarbejdsaftaler med eksterne leverandører, bliver foretaget en revurdering af de implementerede sikkerhedsforanstaltninger.

11. Styring af informationssikkerhedssvagheder, -hændelser og -brud [1]

11.1 Styring af informationssikkerhedshændelser og forbedringer

11.1.1 Rapportering af informationssikkerhedssvagheder

Sikkerhedssvaghed er, når der er faretegn for en potentiel sikkerhedshændelse eller endog sikkerhedsbrud, men som kan lukkes ved afhjælpende foranstaltninger, inden det opstår.

Alle medarbejdere og øvrige personer, der gør brug af it-systemerne, har pligt til at indberette informationssikkerhedssvagheder umiddelbart efter, at disse er konstateret eller der er opstået mistanke om svagheder.

11.1.2 Rapportering af informationssikkerhedshændelser

Sikkerhedshændelse (event) er starten på et sikkerhedsbrud, men som stadig kan håndteres og evt. afværges uden store konsekvenser for forretningen

- Medarbejdere, kommunalbestyrelsesmedlemmer og samarbejdspartnere har pligt til at rapportere sikkerhedshændelser, som observeres i forbindelse med anvendelse af it-systemer og behandling af information.
- Rapportering skal ske hurtigst muligt til It-afdelingens service desk.
- Tyveri eller bortkomst af enhver form for it-udstyr skal omgående meddeles til service desken.

11.1.2 Rapportering af informationssikkerhedsbrud

Sikkerhedsbrud er en fuld sikkerhedshændelse, der ikke kan håndteres og afhjælpes uden at kommunens sikkerhed er blevet kompromiteret med evt. efterfølgende skadevirkninger.

- Alle medarbejdere og øvrige personer, der gør brug af it-systemerne, har pligt til at indberette informationssikkerhedsbrud umiddelbart efter, at disse er konstateret eller der er opstået mistanke om sikkerhedsbrud.
- It-afdelingen udarbejder sammen med ledelsen en fast procedure for håndtering af sikkerhedsbrud.

11.1.4 Erfaring fra informationssikkerhedsbrud

- Projektleder for databeskyttelse er ansvarlig for indsamling, kategorisering og behandling af sikkerhedshændelser og sikkerhedsbrud.

12. Informationssikkerhedsaspekter ved nød, beredskabs- og reetableringsstyring (Beredskabsstyring)

12.1 Informationssikkerhedskontinuitet

12.1.1 Planlægning af informationssikkerhedskontinuitet

- Direktionen er ansvarlig for at fastlægge omfang og rammerne for beredskabsplanen for informationssikkerhed.

12.1.2 Implementering af informationssikkerhedskontinuitet

- Projektleder for databeskyttelse er ansvarlig for, at der udarbejdes en overordnet niveau-II beredskabsplan for informationssikkerhedsområdet.
- It-chefen godkender niveau-II beredskabsplanen for it-området.
- Direktionen er ansvarlig for, at der udarbejdes nødplaner for de kritiske forretningsprocesser.
- Systemejeren er ansvarlig for, at der udarbejdes reetableringsplaner for de kritiske it-systemer.
- Projektleder for databeskyttelse er ansvarlig for, at niveau-II beredskabsplanen er sammenhængende med de tilhørende nødplaner og reetableringsplaner.

12.1.3 Verificer, gennemgå og evaluer informationssikkerhedskontinuiteten

- Projektleder for databeskyttelse gennemgår og om nødvendigt reviderer den niveau-II beredskabsplanen minimum en gang årligt.
- Direktionen sikrer at nødplaner gennemgås og om nødvendigt revideres, minimum en gang årligt.
- Systemejeren gennemgår og om nødvendigt reviderer reetableringsplaner minimum en gang årligt eller ved større ændringer i it-systemet.
- Projektleder for databeskyttelse er ansvarlig for at beredskabsplanen helt eller delvis testes, som en skrivebordstest minimum en gang årligt.
- Projektleder for databeskyttelse er ansvarlig for, at der foretages en evaluering og indføjes eventuelle rettelser til beredskabsplanen med tilhørende dokumenter.

13. Overensstemmelse (Compliance)

13.1 Overensstemmelse med lov - og kontraktkrav

13.1.1 Identifikation af gældende lovgivning og kontraktkrav

- Medarbejderne må alene anvende ophavsretlig beskyttet software og materiale på pc'er, håndholdte enheder og lign, i det omfang der forefindes gyldig licens eller brugsrettigheder til softwaren eller materialet.

13.1.2 Privatlivets fred og beskyttelse af personoplysninger

- Fortrolige personoplysninger skal lagres i fagligt relevante it-systemer, som er godkendte til opbevaring af denne type oplysninger.
- Projektleder for databeskyttelse er ansvarlig for at udbrede kendskabet til, hvordan personoplysninger beskyttes og behandles i overensstemmelse med persondataloven.

13.2 Gennemgang af informationssikkerhed

13.2.1 Uafhængig gennemgang af informationssikkerhed

- Databeskyttelsesrådgiveren foretager en årlig overvågning af kommunens efterlevelse af databeskyttelsesforordningen og databeskyttelseslovens med et rapporteringsmøde med kommunens ledelse.
- It-revisionen vurderer som del af den finanisielle revision en gang årligt, hvorvidt det fastlagte sikkerhedsniveau er implementeret.

13.2.2 Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder

- Direktionen er ansvarlig for at chefer og ledere kontinuerligt sikrer opfølgning på informationssikkerheden inden for eget ansvarsområde.

13.2.3 Undersøgelse af teknisk overensstemmelse

- Projektleder for databeskyttelse sikrer at der foretages en løbende kontrol af de tekniske og administrative sikringsforanstaltninger, ud fra et fastlagt kontrolkatalog.

Frederiksberg Kommunes It-sikkerhedspolitik er senest godkendt af:
Direktionen den 17. december 2019.