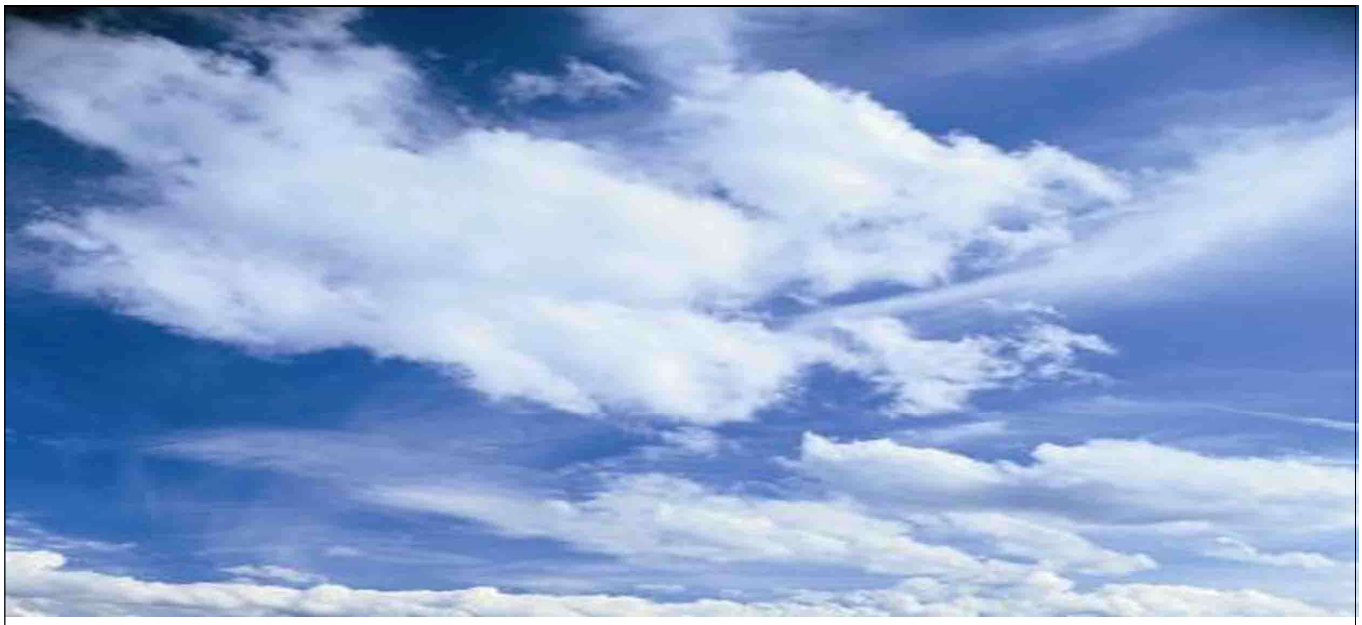

Aabenraa Kommune

Regler for informationssikkerhed

Indholdsfortegnelse

Indledning

Der er foregået tjek ift. Kommunens andre regler, f.eks. ift. Løn og Personale og det er disse regler der henvises til i dokumentet.

Organisation og implementering

Placering af ansvar er vitalt for at sikre opmærksomhed på kommunens informationsaktiver. Organisationsstrukturen i kommunen og samarbejde med eksterne partnere er yderst vigtigt for at opretholde et tidssvarende sikkerhedsniveau. Kontrakter med partnere og andre aftaler er ligeledes et område, der har indflydelse på informationssikkerheden.

Risikobevidsthed

Konsekvensvurdering

Ved ibrugtagning af nye teknologier med høj risiko, skal der foretages en konsekvensanalyse af systemejer

Konsekvenser af hændelser i IT-systemerne skal løbende vurderes af systemejer. Skal dokumenteres i kommunens ESDH-system.

Information om nye trusler, virus og sårbarheder

IT-Afdelingen er ansvarlig for eksternt samarbejde med de fornødne informationskanaler, herunder samarbejde omkring informationssikkerhed med relevante eksterne interessegrupper og sikkerhedsorganisationer.

IT-Afdelingen har etableret en proces for identifikation af nye sårbarheder. Der er udpeget en ansvarlig person eller gruppe for dette jf. beredskabsplanen.

IT-Afdelingen informerer relevante personer i ledelsen om nye trusler, som potentielt kan berøre de pågældende forretningsenheder.

Overordnet risikovurdering

Der gennemføres årligt en bredt funderet risikovurdering af system-/procesejere, der dækker hele organisationen. Målet er at sikre at sårbarheder, trusler og konsekvenser er kendte og at deres sammenhæng afspejles i organisationens risikoprofil.

Risikovurderingen omfatter alle væsentlige processer.

Risikovurdering

Der udarbejdes en detaljeret risikovurdering af systemejer for alle systemer med personoplysninger. Risikovurderingen ligger til grund for frekvensen af fremtidige risikovurderinger samt omfanget af autorisationskontrollen.

Informationssikkerhedspolitik

Offentliggørelse af sikkerhedspolitik

Sikkerhedspolitikken offentliggøres og kommunikeres til alle relevante interessenter, herunder alle medarbejdere. Dette gøres via Medarbejderportalen.

Godkendelse af sikkerhedspolitik

Sikkerhedspolitikken godkendes af Økonomiudvalget hvert andet år.

Opfølgning på implementering af sikkerhedspolitikken

Mindst en gang årligt udfører systemejer en systematisk opfølgning på overholdelse af sikkerhedspolitikken ift. kritiske systemer. Det gælder risikovurdering, autorisationskontrol, kontrol af databehandler.
Hver enkelt leder sikrer løbende, at sikkerhedspolitikken bliver overholdt inden for eget ansvarsområde.

Revision af sikkerhedspolitik

Sikkerhedspolitikken revideres hvert andet år.

Vedligeholdelse af sikkerhedspolitik

Organisationens sikkerhedspolitik, regler, procedurer og tilhørende dokumentation vedligeholdes af øverste sikkerhedsansvarlig og dennes organisation.

Definition af informationssikkerhed og IT-sikkerhed

Definition af IT-sikkerhed

Informationssikkerhed defineres som de samlede foranstaltninger til at sikre fortrolighed, tilgængelighed og integritet. Foranstaltninger inkluderer tekniske, proceduremæssige, lov- og regelmæssige kontroller.

Sikkerhedsimplementering

Kontakt med relevante myndigheder

Ved brud på sikkerheden vurderer DPO'en fra sag til sag, hvordan håndtering af bevismateriale og eventuelt kontakt med relevante myndigheder forløber. Ved politisager, er det politiet, der afgør proceduren for indsamling af bevismateriale.

Ledelsens rolle

Ledelsen skal støtte kommunens informationssikkerhed ved at udlægge klare retningslinier, udvise synligt engagement samt sikre en præcis placering af ansvar.

Sikkerhedsorganisation

Kommunen skal have et informationssikkerhedsudvalg (ISU), der har ansvar for at sikre at informationssikkerheden er synlig, koordineret og i overensstemmelse med kommunens mål.

Koordination af informationssikkerheden

Ansvaret for koordination af sikkerheden på tværs i organisationen varetages af kommunens ISU.

Outsourcing (Hosting, cloud-løsninger mv.)

Ekstern revision af outsourcing partnere

Outsourcing partnere skal sørge for ekstern revision mindst en gang om året.

Outsourcing partnere

Inden indgåelse af aftaler, skal sikkerhedsniveauet ved partneren afklares og sammenlignes med de krav der stilles i sikkerhedspolitikken. Valg af partnere skal godkendes af nærmeste afdelingschef.

Outsourcing

Ved outsourcing af IT-systemer skal IT-Visitationen inden indgåelse af kontrakt indhente information om sikkerhedsniveau fra outsourcing partner og godkende at kommunens sikkerhed samlet set ikke forringes af outsourcing. Informationen dokumenteres i kommunens ESDH-system.

Sikkerhed i tredjeparts adgang

Aftaler om informationsudveksling

Ved udveksling af information og software imellem kommunen og evt. tredjepart skal der foreligge en aftale herom.

Samarbejdsaftaler

For at sikre at kommunens sikkerhedsmålsætning ikke kompromitteres skal ethvert formaliseret eksternt samarbejde være baseret på en samarbejdsaftale.

Indhold af fortrolighedserklæringerne

Definition af de informationer der er omfattet.
En fastlagt løbetid.
Beskrivelse af hvad der skal ske når aftalen udløber.
Underskriverens ansvar for at undgå brud på den aftalte fortrolighed.
Information om omfattede ophavsrettigheder.
Beskrivelse af hvordan informationerne må anvendes, for eksempel hvilke brugsrettigheder til informationerne underskriveren får.
Betingelser for returnering eller destruktion af informationsaktiver ved aftalens ophør.
Erklæringerne dokumenteres i kommunens ESDH-system.

Sikkerhed ved samarbejde med partnere
Ved integration af kommunens systemer og processer med tredjepart skal sikkerhedsrisici altid vurderes og dokumenteres.

Sikkerhedsvurdering af tredjepart
Tredjeparts sikkerhedsniveau skal vurderes imod egen organisations krav. Tredjeparts sikkerhedsdokumentation i form af politik, regler, procedurer og tilhørende dokumenter skal indgå i vurderingen.

Fortrolighedserklæring for tredjepart
Det skal sikres, at tredjepart, der kan få adgang til kommunens data, er omfattet af en fortrolighedserklæring eller databehandleraftale. Erklæringerne dokumenteres i kommunens ESDH-system.

Information til eksterne partnere
Relevante interessenter skal informeres af den ansvarlige for aftalen om krav til efterlevelse af sikkerhedspolitikken i kommunen.

Identifikation, klassifikation og ansvar for aktiver
Informationsaktiver skal beskyttes, uanset om det er fysiske aktiver som dokumenter der er udskrevet, produktionsudstyr eller IT-systemer. Det er derfor nødvendigt at identificere, klassificere og placere ejerskab for alle aktiver.

Håndtering af informationer og aktiver
Procedurer for informationsudveksling
IT- og Digitaliseringschefen har ansvaret for at der skal foreligge retningslinier og procedurer for enhver form for elektronisk informationsudveksling.

Accepteret brug af informationsaktiver
Informationssikkerhedsorganisationen skal lave retningslinier for accepteret brug af kommunens informationsaktiver.

Social Engineering
Medarbejdere skal når de behandler fortrolige informationer være passende opmærksomme på begrebet "social engineering" eller "kunsten at aflure fortrolige informationer uden at blive opdaget". For eksempel kan denne form for bedrag udføres via e-mail, telefon og/eller messenger-/chatprogrammer.

Udskrivning
Printere som benyttes til udskrivning af fortrolige informationer skal placeres i lokaler der ikke er generelt tilgængelige. Hvor det er muligt skal FollowYou anvendes ved udskrivning af personoplysninger

Fortrolige data på mobile enheder
Der må opbevares persondata og fortrolige data på mobile enheder såfremt disse data beskyttes med en adgangskode og i øvrigt følger informationssikkerhedsreglerne ift. opbevaringsperiode.

Opbevaring af fortrolige informationer på privat pc
Der må ikke behandles eller opbevares personhenførbare eller fortrolige informationer på eget udstyr/privat pc, når der arbejdes i Citrix og webmail betragtes det ikke som en privat pc.

Brug af bærbare medier til fortrolige data
Fortrolige informationer skal krypteres, når de opbevares eller transporteres på bærbare medier, f.eks. USB-nøgler.

Udlevering af fortrolige informationer og oplysninger
Fortrolige informationer og oplysninger må udleveres, hvis der foreligger underskrevne fortrolighedsaftaler.
Personhenførbare og fortrolige oplysninger må kun udleveres til bemyndigede personer. Dokumentation opbevares i kommunens ESDH-system.

Opbevaring af fysiske dokumenter
Skriveborde skal ryddes for dokumenter med personoplysninger og fortrolige oplysninger senest ved arbejdsdagens afslutning.
Dokumenter med personhenførbare oplysninger må ikke ligge med forsiden opad når du forlader dit skrivebord i arbejdstiden.

Ejere af systemer og data

Ansvar for adgangsrettigheder
Systemejer har ansvaret for at fastlægge og løbende revurdere adgangsrettigheder.

Ejerskab
Alle informationsaktiver skal have udpeget en ejer.

Administration af internet-domænenavne
Der skal forefindes en liste over kommunens registrerede domænenavne, status for brug, betalingsoplysninger og dato for fornyelse. Listen kan trækkes fra vores certifikatløsning.

Sikkerhedsansvar for IT-funktioner

Alle kritiske IT-funktioner der kræver specialviden, færdighed eller erfaring skal identificeres, og der skal udpeges en driftsansvarlig ejer. Dokumentationen skal opbevares i kommunens ESDH-system.

Sikkerhedsansvar for informationsaktiver

Den daglige sikkerhedsansvarlige har ansvar for at vedligeholde en liste over samtlige informationssystemer. Listen angiver den ansvarlige ejer af hvert enkelt system (KITOS).

Dataintegritet

Opbevaring og behandling af data

Forretningskritiske data skal altid opbevares og behandles således, at dataintegriteten ikke kan drages i tvivl.

Personalesikkerhed og brugeradfærd

Informationssikkerheden i kommunen afhænger i høj grad af medarbejderne. Det er nødvendigt at sikre kommunen gennem ansættelse af de rigtige medarbejdere, uddanne medarbejdere i jobfunktioner og sikkerhed, medarbejderne skal bl.a. øve sig i informationssikkerhed (e-learning og sikkerhedsfilm) - samt sætte regler for, hvordan man skal agere i forhold til sikkerhedshændelser og -risici.

Ansættelsesprocedurer

Returnering af aktiver ved fratrædelse jfr. tjekliste der er udarbejdet og ligger på Medarbejderportalen

Medarbejderen skal aflevere alle udleverede effekter ved samarbejdets ophør.

Ansættelsesaftalen skal indeholde og uddybe:

Henvisning til overenskomst, GDPR og informationssikkerhedspolitik.

Aftale om ansættelse

Faste og midlertidige medarbejdere modtager ansættelseskontrakt i e-Boks, såfremt der ikke reageres inden for 8 dage, betragtes ansættelseskontrakten som accepteret.
Lederen informerer om informationssikkerhedspolitikken og hvad det betyder i forhold til den konkrete ansættelse.

Baggrundscheck af medarbejdere kan omfatte:

Personlig og/eller faglig reference.
Ansøgerens curriculum vitae.

Uddannelser og professionelle kvalifikationer.
Straffe- og/eller Børneattest på områder hvor det fremgår at man skal indhente attester. Straffe- og/eller børneattest gemmes på personalesagen.

Verifikation af erfaring og uddannelse
Personaleafdelingen er ansvarlig for gennemgang og kontrol af om formel uddannelsesbevis, og dokumentation for erfaring foreligger.

Baggrundscheck af eksterne konsulenter
Den enkelte leder skal sikre, at der sker forsvarligt baggrundscheck af eksterne konsulenter. Det kan f.eks. være referencer fra andre kunder, Garanti fra virksomheden, hvor vedkommende er ansat mv. Dette skal ske på baggrund af en risikovurdering – ved adgang til fortrolige eller følsomme oplysninger, skal risikovurderingen dokumenteres.

Baggrundscheck af medarbejdere
Den enkelte leder skal sikre, at der sker forsvarligt baggrundscheck af medarbejdere med ansvar for forretningskritiske arbejdsområder. Det kan alene ske ved at indhente referencer, og på de områder hvor det er besluttet at der må indhentes børne- og/eller straffeattest, kan disse indhentes.

Funktionsadskillelse

Adgang til produktionsdata
Systemadministratorers adgang til fortrolige oplysninger skal begrænses og registreres.

Sikring af forretningskritiske systemer
Forretningskritiske systemer skal beskyttes ved hjælp af funktionsadskillelse, således at risikoen for misbrug af privilegier minimeres. Listen over forretningskritiske systemer findes i bilag 2 i SLA'en.

Ledelsens ansvar

Det er nærmeste leders ansvar at alle medarbejdere:
Er tilstrækkeligt informeret om deres roller og ansvar i forbindelse med sikkerhed, før de tildeles adgang til kommunens systemer og data.
Er gjort bekendt med regler og retningslinier, således at de kan leve op til kommunens informationssikkerhedspolitik.
Er motiverede til at leve op til kommunens informationssikkerhedspolitik og retningslinier.
Opnår et opmærksomhedsniveau i spørgsmål vedrørende informationssikkerhed, der er i overensstemmelse med deres roller og ansvar i kommunen.
Holder sig inden for de retningslinier og bestemmelser, der er for ansættelsen, inkl. kommunens informationssikkerhedspolitik og konkrete arbejdsmetoder.

Uddannelse

Sikkerhedsuddannelse for IT-medarbejdere

Alle IT-medarbejdere skal specifikt uddannes i sikkerhedsaspekter for at minimere risikoen for sikkerhedshændelser.

Uddannelse i sikkerhed skal opdateres med kursus/workshop/træning med sikkerhedsindhold efter behov.

Uddannelse

Uddannelse i sikkerhedspolitikken

Det er den nærmeste leder der har ansvaret for følgende:

Alle nye medarbejdere skal i starten af deres ansættelse modtage kommunens informationssikkerhedspolitik.

Alle medarbejdere skal have træning i kommunens informationssikkerhedspolitik og baggrundsviden omkring denne

Sanktionsmuligheder og anmeldelse af ulovligheder

Sanktioner

De ansættelsesretlige regler er gældende.

Overtrædelse af sikkerhedsreglerne

For medarbejdere, der bryder kommunens politikker, regler eller retningslinjer for informationssikkerhed gælder de ansættelsesretslige regler, omkring tilrettevisende samtaler, advarsel, afsked og bortvisning alt efter graden af forseelsen.

Adfærdsregler for brug af adgangskode

Brug af kodeordsbeskyttet pauseskærm

Som bruger skal du aktivere kodeordsbeskyttet skærmlås når du forlader din arbejdsstation og den er uden for din synsvidde.

Brug af autologin funktioner

Automatisk login eller systemer hvor kodeord gemmes i genveje eller på funktionstaster må ikke benyttes.

Overdragelse af kodeord

Det er ikke tilladt for medarbejderen at udlevere sin kode. IT-Helpdesk kan udlevere midlertidig kode til dig, verbalt, f.eks. over telefonen, i tilfælde af at du har glemt din kode.

Genbrug af kodeord

Det er ikke tilladt at genbruge det samme kodeord på interne og på eksterne systemer.

Kodeord er strengt personlige

Kodeord er strengt personlige og må ikke deles med andre.

Adfærdsregler for brug af internet

Download af filer fra internet

Filer må downloades fra internet i begrænset arbejdsmæssigt omfang.

Download af programmer fra internet

Det er kun tilladt at hente programmer fra Google Play Store, App Store og tilsvarende anerkendte kilder.

Afvikling af programmer i forbindelse med internetsurfing

Det er tilladt at afvikle browserbaserede programmer, for eksempel netbank-programmer, forudsat sikkerhedspolitikken i øvrigt overholdes.

Terminalsessioner til fjernstyring

Godkendt personale må tilgå visse systemer over internet, hvis disse sikres på forsvarlig vis. Adgang skal tillades af den sikkerhedsansvarlige i samråd med systemejerne.

Sikkerhedsindstillinger i web-browser

Der må kun anvendes forud installerede, godkendte webbrowsere. Brugerne må ikke forsøge at omgå eller bryde sikringsforanstaltningerne.

Medarbejderes private brug af internetadgang

Kommunens internetadgang må også anvendes til privat formål, såfremt loven og sikkerhedspolitikken i øvrigt overholdes, og såfremt arbejdsrelateret brug ikke generes på nogen måde.

Adfærdsregler for brug af e-mail

Elektronisk udveksling af post og dokumenter

Hvis e-mail bruges til bindende aftaler skal de journaliseres i kommunens ESDH-system.

Opbevaring og sletning af e-mail

E-mail der indeholder følsomme eller fortrolige personoplysninger, skal journaliseres og/eller slettes efter senest 30 dage.

Fortrolig e-mail

E-mail med følsomt indhold skal krypteres med godkendt software, f.eks. Digital Post og Send Sikkert. Dette gælder især for fortrolig information eller følsomme personoplysninger der sendes over internet.

Phishing og bedrageri

Uanset at kommunen udfører indholdsscanning af alle e-mails, skal brugere skal være opmærksomme på "phishing" og "social engineering"; der for eksempel kan betyde, at de kan modtage tilsyneladende oprigtige e-mails der forsøger at franarre personlige eller fortrolige oplysninger, eller forsøger at få brugeren til at foretage uønskede handlinger.

Medarbejderes private brug af e-mail

Kommunen tillader brug af e-mail-systemer også til privat brug, såfremt sikkerhedspolitikken i øvrigt overholdes, herunder at opbevaring af personoplysninger ikke må overskride 30 dage.

Vedhæftede filer

Kun dokumentfiler og billedfiler må vedhæftes og åbnes. IT-Afdelingen justerer løbende, hvilke filtyper, der kan vedhæftes jf. risikovurderingen.

Sagsbehandling og journalisering af e-mail

Modtaget og afsendte e-mails skal journaliseres og behandles efter gældende lovgivning.

Adfærdsregler for brug af messenger-programmer

Autentificering

Brugere skal være opmærksomme på, at messenger-programmer anvender svag autentificering. Det vil sige, brugeren har sjældent eller aldrig vished for, hvem der kommunikeres med.
Derfor må disse programmer ikke anvendes i arbejdsøjemed.

Adfærdsregler for brug af sociale netværk

Overvågning af sociale netværk

Som led i den almindelige netværksovervågning bliver netværkstrafik til sociale netværk også overvåget.

Brug af 3.-parts applikationer på sociale netværk

Du må ikke anvende 3.-parts-applikationer på kommunens IT-systemer.

Kommunens informationer på sociale netværk

Bortset fra offentlige informationer, må kommunens informationer aldrig deles på et socialt netværk. Kommunens informationer, f.eks. præsentationer, billeder og film, må ikke offentliggøres på sociale netværk, hvor der kan være tvivl om, hvorvidt kommunen bevarer sin ophavsret til informationerne.

Sociale netværk med forretningsforbindelser

Du må gerne "connecte" eller "være ven" med samarbejdspartnere på sociale netværk, forudsat at sikkerhedspolitikken i øvrigt overholdes.

Omfang af brug af sociale netværk

Privat brug af sociale netværk skal fortrinsvis lægges uden for almindelig arbejdstid eller i pauser.

Brugere af sociale netværk skal være specielt opmærksomme på at:

Personer på sociale netværk er ikke altid dem de udgiver sig for at være (det er ikke sikkert den person du tror er en kollega faktisk er det).

Persondata må aldrig deles på sociale netværk.

Download af filer som du modtager via et socialt netværk er underlagt de samme regler som øvrige downloads.

Informationer som du har lagt ud på et socialt netværk, kan aldrig trækkes tilbage.

Du vil med stor sandsynlighed opleve at nogen forsøger at franarre dig dine bruger-id'er og/eller dine adgangskoder (phishing).

De sociale netværk, som du bruger, registrerer og gemmer oplysninger om dig og de informationer du søger.

Blokering af sociale netværk

IT-Afdelingen skal blokere brugernes adgang til sider, der udgør en risiko for netværket.

Anvendelse af sociale netværk

Godkendte sociale netværk må gerne anvendes fra virksomhedens IT-systemer.

Adfærdsregler for brug af trådløse netværk

Installation af trådløst udstyr

Medarbejdere må installere og bruge udstyr, forudsat at IT-Afdelingen har godkendt det.

Forbindelse til åbne trådløse netværk

Medarbejdere må ikke forbinde deres mobile udstyr til åbne trådløse netværk.

Fysisk sikkerhed

Rådhuset er åbent for alle i dagtimerne jf. politisk beslutning. Særlige områder, blandt andet serverrum, skal være aflåste 24 timer i døgnet.

Generelle retningslinier

Sikring af kontorer, lokaler og udstyr

Den øverste sikkerhedsansvarlige må uddelegere ansvaret for at sikre en passende fysisk sikring af kontorer, rum og udstyr bliver implementeret og vedligeholdt.

Aflåsning af lokaler og bygninger

Alle vinduer skal være lukket når du forlader kontoret.

Dokumenter med personoplysninger skal være forsvarligt opbevaret, enten i aflåste skabe/skuffer eller bag en låst dør.

Tekniske sikringsforanstaltninger

Brandsikring

Passende brandsikringsudstyr jf. arbejdsmiljøreglerne skal forefindes, og være korrekt placeret.

Køling

Alle serverrum skal sikres med veldimensioneret airconditionanlæg.

Nødstrømsanlæg

Alle forretningskritiske systemer skal beskyttes med nødstrømsanlæg til at sikre hurtig og korrekt systemnedlukning i tilfælde af strømudfald.

Beskyttelsesanlæg

Miljømæssig sikring af serverrum

Serverrum skal på forsvarlig vis sikres mod miljømæssige hændelser som brand, vand, eksplosion og tilsvarende påvirkninger.

Udstyrssikkerhed

Forsikringsdækning for mobile enheder

Forsikringskontoret skal sikre at der er etableret passende forsikringsdækning i forbindelse med opbevaring og anvendelse af IT-udstyr uden for kommunens lokaliteter.

Afskaffelse eller genbrug af udstyr

Når udstyr bortskaffes eller genbruges skal kritiske/følsomme informationer og licensbelagte systemer fjernes eller overskrives. Dokumentation af destruering gemmes i kommunens ESDH-system.

Sikring af hjemmearbejdspladser

Hjemmearbejdspladser og deres kommunikationsforbindelser skal beskyttes i forhold til de informationer og forretningssystemer, de benyttes til.

Vedligeholdelse af udstyr og anlæg

IT-Drift skal sikre vedligeholdelse af udstyr i dialog med systemejer og leverandør.

Kun godkendte leverandører må udføre reparationer og vedligeholdelse jf. garantiaftaler.

Reparationsvirksomheden skal overholde fornødne sikkerhedskrav hvis udstyr repareres eller vedligeholdes uden for kommunens lokaliteter.

Kritiske/følsomme informationer skal slettes fra udstyr der repareres eller vedligeholdes uden for kommunens lokaliteter.
IT-Afdelingen er ansvarlig for at leverandøren fører log over alle fejl og mangler jf. SKI-kontrakt.

Sikring af kabler
Kabler til datakommunikation skal beskyttes mod uautoriserede indgreb og skader.
Faste kabler og udstyr skal mærkes klart og entydigt.

Forsyningssikkerhed
Byråds- og Direktionssekretariatet har ansvaret for, at alle forsyninger som elektricitet, vand, kloak, varme, og ventilation har den fornødne kapacitet og løbende inspiceres for at forebygge uheld der kan have indflydelse på informationsaktiverne.
Data-og telekommunikationsforbindelser skal etableres via minimum to adgangsveje for forretningskritiske systemer.

Spisning i nærheden af udstyr
Der må ikke spises og drikkes i nærheden af forretningskritisk udstyr.
Der må ikke spises og drikkes i serverrum.

Placering af udstyr
Udstyr der benyttes til at behandle kritiske/følsomme informationer skal placeres så informationerne ikke kan ses af uvedkommende.
IT-Afdelingen skal begrænse fysisk adgang til gateways og trådløse adgangspunkter.
Der må ikke tages billeder af serverrum.

Tyverimærkning af IT-udstyr
Alt udstyr undtaget mobiltelefoner skal være tydeligt mærket for at minimere risikoen for tyveri.
Opmærkningen foretages af IT-Helpdesk

Fjernelse af udstyr fra kommunens lokaliteter
Udstyr må kun fjernes fra kommunens lokaliteter, hvis der foreligger en aftale med nærmeste leder.
Ved afhentning af udstyr i IT-Helpdesk, kvitteres der for modtagelse.

Registrering af IT-udstyr
Alt IT-udstyr bestilt via TopDesk skal registreres i inventarlisten, med opgavenummer, EAN og rekvirenten. IT-afdelingen kan trække alle oplysninger om PC'ere (Stationær og bærbar) via et program og derigennem dokumentere placering og ejerskab.

Opsyn med mobile enheder

Mobile enheder må ikke efterlades uden opsyn i uaflåste rum eller synligt i bilen.
Adgang til data på bærbare computere skal beskyttes med et login password.

Brug af mobile enheder

Bærbart udstyr skal medbringes som håndbagage under rejser.
Bærbart udstyr må ikke udlånes til venner, familie eller kollegaer.

IT- og netværksdrift

Vedligeholdelse og opdatering af IT-systemer er nødvendigt for at opretholde et passende sikkerhedsniveau for kommunen. Drift af IT-systemer inkluderer elementer af overvågning af systemernes helbredstilstand, opdatering og sikkerhedskopiering af data. De fleste IT-systemer i dag er afhængige af netværk, og derfor er administration, opbygning, sikring og vedligeholdelse af netværk vitalt for kommunen. Den trussel, som uautoriseret adgang indebærer, gør det nødvendigt med klare regler for brugen af kommunens netværk samt overvågning af infrastrukturen. Reglerne forefindes i IT-Drift på drev og krypterede USB-nøgler.

Daglig administration

Systemer til styring af adgangskoder

Så vidt muligt skal der benyttes IT-systemer, der automatisk kan styre de krav, der findes til adgangskoder i afsnittet "Adgangskoder og metoder"

Firewall-funktioner på servere

Alle servere skal benytte firewalls til at sikre at der kun gives adgang til nødvendige services.

Afprøvning af procedurer for sikkerhedskopiering

Muligheden for at retablere data fra backup-systemer skal regelmæssigt testes i et testmiljø. Endvidere skal retablering testes efter system- eller proces-ændringer, der kan påvirke backup-rutiner.
Dokumentationen ligger i kommunens ESDH-system.

Ekstern serviceleverandør

Netværksleverandøren skal kunne levere:

De nødvendige teknologiske muligheder for autentifikation, kryptering og overvågning.
De nødvendige tekniske opsætninger til at sikre opkoblinger i overensstemmelse med samarbejdsaftalen.
Adgangskontrol der sikrer mod uvedkommendes adgang.

Overvågning af serviceleverandøren

IT-Afdelingen skal regelmæssigt overvåge serviceleverandørerne, gennemgå de aftalte rapporter og

logninger samt udføre egentlige revisioner for at sikre, at aftalen overholdes, og at sikkerhedshændelser og -problemer håndteres betryggende. Dokumentationen ligger i kommunens ESDH-system.

Håndtering af datamedier

Beskyttelse af systemdokumentation

IT-Afdelingen skal opbevare systemdokumentation passende sikkert. Systemdokumentationen opbevares på drev og kun medarbejdere med administratorrettigheder har adgang.
Adgangsrettigheder til systemdokumentation skal holdes på et minimum og godkendes af IT-chefen.

Forretningsgangen for beskyttelse af datamediers indhold skal omfatte:

Håndtering og mærkning.
Adgangsbegrænsning.
Log over tildelte autorisationer.
Afstemningsprocedurer.
Beskyttelse af midlertidigt lagrede data.
Fysiske krav til opbevaringssted, fx temperatur og luftfugtighed ifølge leverandørens specifikationer.
Minimering af distribution.
Klar mærkning af alle kopier.
Regelmæssig gennemgang af distributions- og autorisationslister.

Beskyttelse af følsomme og fortrolige data på datamedier

IT-Afdelingen skal etablere procedurer, der sikrer datamediers indhold mod uautoriseret adgang og misbrug af mediernes indhold. Proceduren omfatter adgangstyring på Citrix og VPN.

Brug af datamedier

Benyttelse af mobile datamedier skal være krypteret og forretningsmæssigt begrundet.

Opbevaring af datamedier

Systemejer/afdelingschefer skal sikre at medierne eller informationerne på mediet opbevares og slettes i henhold til gældende lovgivning.

Virusscanning af mobile datamedier

Inden ibrugtagning skal ethvert datamedie scannes for virus. Ved indsættelse i PC bliver datamedier scannet automatisk.

Lagring og adgangsrettigheder til systemdokumentation

Systemdokumentation opbevares i mindst 5 år efter endt brug.

Afskaffelse og genbrug af medier

Alle datamedier, for eksempel harddiske, SSD'er, USB-nøgler og andre hukommelsesenheder, skal sikkerhedsslettes eller destrueres inden bortskaffelse.

Der skal være retningslinier for de enkelte datamediers destruktionsmetode jf. aftale med KIS.

Sletning skal foregå i overensstemmelse med procedure for sikkerhedssletning jf. aftale med hhv. KIS og CJU.

Destruktion af følsomme, fortrolige eller kritiske data skal logges af hensyn til kontrolsporet.

Operationelle procedurer og ansvarsområder

Adskillelse af test og drift

Testmiljøer skal være systemteknisk eller fysisk adskilt fra driftsmiljøet.

Driftsafviklingsprocedurer

Driftsafviklingsprocedurer for forretningskritiske systemer skal være dokumenterede i kommunens ESDH-system, ajourførte og tilgængelige for driftsafviklingspersonalet og andre med et arbejdsbetinget behov.

Sikkerhedskopiering af data på serversystemer

IT-Afdelingen er ansvarlig for opbevaring og sikkerhedskopiering af alle forretningskritiske informationer på serversystemer.

Større operativsystemopdatinger, for eksempel "service packs".

Større opdateringer skal testes grundigt for kompatibilitet med anvendte applikationer inden opdateringerne installeres i produktionsmiljøet.

Antivirusprodukter på servere

Der skal være installeret antivirus beskyttelse på alle systemer, hvor dette er muligt.

Programpakkeopdateringer, for eksempel "service packs".

Alle opdateringer skal testes i et testmiljø inden opdateringerne installeres i produktionsmiljøet.

Driftsansvar

IT-Afdelingen er ansvarlig for drift, administration og sikkerhed af IT-systemer der bliver driftet in-house. Herunder efterlevelsen af sikkerhedspolitikker, regler og procedurer.

Rettelser til applikations-programpakker

IT-Afdelingen skal løbende vurdere tilgængelige sikkerhedsrettelser, for eksempel "patches" eller "hot-fixes", til anvendte programpakker. Udrulning/installation på relevante systemer skal så vidt muligt foretages i servicevinduer efter vurdering og positiv funktions- og kompatibilitetstest.

Rettelser til operativsystemer
IT-Afdelingen skal løbende vurdere tilgængelige sikkerhedsrettelser, for eksempel "patches" eller "hot-fixes", til anvendte operativsystemer. Udrulning/installation på relevante systemer skal foretages i servicevinduer efter vurdering og positiv funktions- og kompatibilitetstest.

Softwareopdateringer generelt
IT-Afdelingen skal forestå installation af alle større programrettelser, når det vurderes, at disse har positiv indflydelse på den samlede sikkerhed.
Systemejere er ansvarlige for, at der løbende sker regelmæssig opdatering af anvendt hosted software.
IT-Drift er ansvarlig for, at der løbende sker regelmæssig opdatering af in-house software.

Dokumentation
Systemejere skal sikre at alle systemer er dokumenterede, ved at dokumenterer jævnfør kommunens standard for minimumsregistrering i KITOS.

Opbevaring af sikkerhedskopier på ekstern lokation
Datamedier til reetablering af forretningskritiske systemer skal opbevares uden for kommunens lokaliteter.

Systemplanlægning

Integration af informationssystemer
Hvis integration af informationssystemer (hjemmesider, medarbejderportalen, pyloner mv.) resulterer i en forøget risiko så skal denne vurderes og godkendes af systemejer.

Kapacitetsplanlægning
IT-systemernes dimensionering skal afpasses efter kapacitetskrav. Belastning skal overvåges således at opgradering og tilpasning kan finde sted løbende. Dette gælder især for systemer, der er kritiske for kommunens virksomhed.

Sikkerhed i systemplanlægning
Ved planlægning af systemer skal sikkerhedsbetragtninger altid medtages i overvejelserne.
IT-Sikkerhedskrav skal tages i betragtning ved design, test, implementering og opgradering af nye IT-systemer og ved systemændringer.

Overvågning af systemer

Tilgængelighedshændelser
Hændelser der har indflydelse på tilgængelighed skal afklares i henhold til gældende driftsaftaler (SLA).

Driftshændelser der ikke kan afklares inden for aftalt tid, skal udløse procedurer for hændelseshåndtering. Information til brugerne sker jf. SLA.

Kapacitetsovervågning
Alle serversystemer med kritiske informationer skal løbende overvåges for tilstrækkelig kapacitet til at sikre pålidelig drift og tilgængelighed.

Registrering af driftsstatus
IT-Drift skal registrere væsentlige forstyrrelser og uregelmæssigheder i driften af systemerne. Dokumentationen ligger i kommunens ESDH-system.

Overvågning af tilgængelighed
IT-Drift skal løbende overvåge alle forretningskritiske IT-systemer og regelmæssigt dokumentere systemernes tilgængelighed.

Styring af ændringer

Sikring af kritiske data
IT-Drift skal ændre standardadgangskode efter installation af et nyt system.

Godkendelse af nye eller ændrede systemer
IT-Drift skal etablere en godkendelsesprocedure for nye systemer, for nye versioner og for opdateringer af eksisterende systemer samt de afprøvninger, der skal foretages, inden de kan godkendes og sættes i drift.

Styring af ændringer hos serviceleverandøren
IT-Drift skal sikre, at ændringsstyring af serviceleverandørens ydelser følger samme retningslinier som kommunens egen.

Planlægning, test og godkendelse af ændringer
Ændringer skal planlægges og afprøves inden de sættes i drift.

Retningslinier for ændringer
Ændringer skal kun gennemføres når de er forretningsmæssigt velbegrundede.
IT-Drift har ansvaret for at der foregår en entydig identifikation og registrering af væsentlige ændringer. Dokumentationen findes på drev og krypteret USB-nøgler.
IT-Drift har ansvaret for at der findes en nødprocedure til at mindske effekt fra fejlslagne ændringer. Dokumentationen findes på drev og krypteret USB-nøgler.

Sikring af serversystemer

Servere skal sikres og testes inden implementering i produktionsmiljøet. Jf. kravspec og designspec.

Ændringer i forretningskritiske systemer

Alle ændringer i forretningskritiske systemer udføres efter godkendt procedure. Alle procedurer skal indeholde en alternativ plan til reetablering af det forretningskritiske system. Vilkårene for aktivering af den alternative plan skal ligeledes fremgå af proceduren. Dokumentationen findes på drev og krypterede USB-nøgler.

Forbudte og tilladte programmer

IT-Drift skal vedligeholde en liste over godkendte og forbudte programmer. Dokumentationen ligger på drev.

Krav til indstillinger af internet-browser

I Citrix skal browsere altid være konfigureret til medium sikkerhed eller højere sikkerhedsindstillinger. Lokalt installerede browsere skal følge gældende retningslinjer i SLA for IT-Afdelingen.

Installation af programmer på arbejdsstationer

Medarbejderne må installere programmer på kommunens arbejdsstationer jf. SLA.

Beskyttelse mod skadelige programmer

Adware

Adware-beskyttelse baseres på medarbejder-"awareness", sikkerhedsindstillinger i internetbrowser, begrænsninger i brugeres muligheder for softwareinstallation i Citrix samt brug af adware-scannere.
IT-Drift skal sikre at der regelmæssigt scannes for adware på alle arbejdsstationer.

Spyware

Installation af spyware søges undgået gennem begrænsningerne i muligheder for softwareinstallation.
Installation af spyware søges undgået gennem patch-management-processer.
IT-Drift skal sikre at der regelmæssigt scannes for spyware på alle arbejdsstationer.

Kontrol af antivirus på arbejdsstationer

Medarbejdere skal på eget udstyr til brug for hjemmearbejde løbende kontrollere, at anti-virus er aktivt på deres computere og at definitionerne ikke er over én uge gamle.
IT-Drift sikrer tilsvarende på administrative arbejdspladser.

Antivirus-produkter på arbejdsstationer

IT-Drift skal sikre, at der er installeret aktive antivirus-produkter på samtlige computere på kommunens lokaliteter, og at disse opdateres højst et døgn efter leverandørens opdateringer.

Indholdsfiltrering

Automatisk indholdsfiltrering

Systemerne skal jævnligt scannes for spammail og phishing. Disse mails mv. skal sættes i karantæne automatisk.

Spam-mail beskyttelse

Kommunen bortfiltrerer e-mail, der opfylder kommunens kriterier for spam-mails.
Medarbejderne skal udvise forsigtighed med deres brugeridentitet i forbindelse med videregivelse af eksempelvis mailadresser, samt i forbindelse med modtagelsen af uønskede e-mails.

Styring af netværk

Rutekontrol

IT-Drift skal begrænse routing imellem forskellige netværkssegmenter således at kun nødvendig trafik videresendes.

Opdeling af netværk

IT-Drift skal segmentere netværk for at etablere en passende adskillelse imellem forskellige tjenester, brugergrupper eller systemer.
Mindstekrav til netværkssegmentering er at IT-Drift etablerer en "demilitariseret zone" (DMZ) hvor offentligt tilgængelige servere placeres adskilt fra internt tilgængelige servere.

Beskyttelse af diagnose- og konfigurationsporte

Fysisk og logisk adgang til diagnose- og konfigurationsporte skal kontrolleres.

Sikring af netværk

IT-Drift har det overordnede ansvar for at beskytte kommunens netværk.

Tilslutning af udstyr til netværk

Andre medarbejdere eller konsulenter må ikke koble udstyr sammen med det interne netværk. Kun IT-Drift må koble udstyr på det interne netværk.

Fjernstyring og administration

Det er tilladt at benytte værktøjer til fjernadministration, hvis der foreligger sikkerhedsgodkendelse af produktet. Listen over sikkerhedsgodkendte produkter findes i kommunens ESDH-system.

Hjemmearbejde

Tillades når sikkerhedspolitikken i øvrigt overholdes.

Der må kun gives adgang til sikkerhedsgodkendte systemer igennem Citrix.

Installation af netværksudstyr

Det er ikke tilladt at installere netværksudstyr uden forudgående sikkerhedsgodkendelse.

Sikkerhedsgodkendelsen fremlægges af leverandøren og dokumenteres i kommunens ESDH-system sammen med fortrolighedserklæringerne.

Adgang til aktive netværksstik

Adgang til aktive netværksstik skal styres af IT-Drift.

Trådløse netværk

Adgang til trådløse netværk for gæster

Der stilles åbent gæstenet til rådighed for gæster og borgere.

Gæsters brug af kommunens trådløse netværk

Netværket kan kun anvendes til internetadgang og giver ikke adgang til interne systemer.

Adgang til administrative trådløse netværk

Brugere skal autentificeres ved hjælp af et certifikat før der gives adgang til kommunens administrative trådløse netværk. For eksempel ved hjælp af IEEE 802.1x.

Placering af trådløse netværk

Trådløst udstyr må kun forbindes til den eksisterende infrastruktur ved hjælp af firewall.

Brug af trådløse lokalnetværk

Kommunens trådløse netværk betragtes som sikre, beskyttede netværk.

Forbindelser med andre netværk

Brug af automatisk identifikation af netværksudstyr

IT-Drift skal etablere automatisk identifikation af netværksenheder på netværkssegmenter, hvor det er væsentligt, at kommunikationen kun må ske fra specifikt udstyr eller specifik lokation.

Indkommende netværksforbindelser

Der tillades kun etablering af forbindelser fra internet til sikkerhedsgodkendte servere - eksempelvis til e-mail- og web-servere.

Mobile enheders tilslutning til andre netværk

Det er tilladt at forbinde mobilt udstyr til andre lukkede netværk.

Netværksovervågning

Overvågning af netværk

IT-Drift er ansvarlig for kontinuerligt at overvåge brugen og sikkerheden af kommunens netværksinfrastruktur. IT-Drift er ansvarlig for identificering, diagnosticering, løsning og rapportering af hændelser, samt for samarbejde med andre interessenter.

Overvågning af internet-brug

Kommunen filtrerer og begrænser internetadgang.

Overvågning af internetforbindelser

IT-Drift skal løbende overvåge internetforbindelser med henblik på at detektere elektroniske angreb. IT-Drift skal sikre, at logfiler tilgår kommunens SIEM-løsning mhp. automatiseret gennemgang. og mindst 3 måneders historik skal opbevares.

Overvågning af systemadgang og brug

Opbevaring af opfølgningslog

IT-Drift skal opbevare log for sikkerhedshændelser på væsentlige systemer i mindst 3 måneder.

Fejllog

Fejl skal logges og analyseres, og nødvendige udbedringer dokumenteres og forholdsregler skal gennemføres.

Administratorlog

Aktiviteter udført af systemadministratorer og -operatører samt andre med særlige rettigheder skal logges.

Beskyttelse af log-oplysninger

Log-faciliteter og log-oplysninger skal beskyttes mod manipulation og tekniske fejl.

Opfølgningsloggen skal så vidt muligt indeholde:

Brugeridentifikation.*****

Dato og klokkeslæt for væsentlige aktiviteter.*****

Identificering af arbejdsstation eller netværksenhed.*****

Registrering af systemadgange og forsøg herpå.*****

Registrering af dataadgange og forsøg herpå.*****

Ændringer i systemkonfigurationen.*****

Brug af særlige rettigheder, for eksempel privilegerede eller administratorrettigheder.

Brug af hjælpeværktøjer.

Brug af benyttede datafiler.

Anvendte netværk og protokoller.*****

Alarmer fra adgangskontrolsystem.

Aktivering og deaktivering af beskyttelsessystemer.

Hændelsestype.*****

Angivelse af om hændelsen lykkedes eller fejlede.

Hændelsens oprindelse.

Navn eller identitet på den anvendte data, systemkomponent, eller ressource.*****

Emnerne markeret med ***** er minimumskrav

Opfølgningslogning

IT-Afdelingen skal logge sikkerhedshændelser på kommunens systemer.

Hændelseslogning

Alle produktionssystemer skal logge information om adgang og forsøg på adgang, for at kunne spore uautoriseret aktivitet.

Logfiler skal så vidt muligt integreres i kommunens SIEM løsning, således de bliver gennemgået automatisk vha. de opsatte regler. Det er IT-Drift, der sikrer at reglerne løbende er tilpasset den aktuelle trusselssituation.

Alle sikkerhedshændelser skal logges og opbevares i minimum 3 måneder af hensyn til opfølgning på adgangskontroller og eventuel efterforskning af fejl og misbrug.

Mobile arbejdspladser og hjemmearbejdspladser

Sikkerhedskontroller overfor fjernopkoblet udstyr.

IT-Helpdesk skal sikre, at bærbare PC'ere bliver sikret med antivirus og adgangskontrolsystemer. Disse foranstaltninger skal opdateres løbende. Mobiler og tablets bliver ikke sat op af IT-Helpdesk.

Antivirusprogrammer

IT-Helpdesk skal sikre, at antivirusprogrammer er installeret på PC'ere udleveret af IT-Helpdesk.

Softwaren skal altid holdes opdateret.

Adgang til netværket

Netadgang og systemadgang begrænses ved brug af firewalls.

Adgang til data på kommunens netværk

Ved fjernadgang til data på kommunens netværk, må der ikke gemmes data på lokale harddiske eller andre eksterne medier.

Adgang til applikationer på kommunens netværk

Der gives kun adgang til applikationer i Citrix, som er godkendt af IT-Afdelingen.

Elektroniske forretningsydelser

Offentlig tilgængelig information

Det er IT-Afdelingens ansvar, at offentlig tilgængelig information, f.eks. på kommunens webservere, er passende beskyttet mod uautoriserede ændringer.

Online transaktioner

Online transaktionssystemer skal beskyttes særligt, især hvis eksterne brugere tilbydes mulighed for direkte at opdatere i kommunens databaser. IT-Afdelingen skal præcisere de nødvendige krav.

Brug af kryptografi

Nøglehåndtering

IT-Helpdesk skal etablere et nøglehåndteringssystem, som understøtter kommunens anvendelse af kryptografi.

Godkendelse af krypteringsprodukter

IT-Visitationen skal godkende alle produkter der indeholder kryptografi, før disse må benyttes til fortrolige data.

Kryptering af administrative netværksforbindelser

Netværksforbindelser, der benyttes til IT-administration skal altid krypteres. Dette betyder alt udstyr undtagen terminaler med direkte forbindelse.

Kryptering af filer

Fortrolige- og følsomme personoplysninger skal altid opbevares i fagsystemer eller kommunens ESDH system.

Brug af kryptering i forbindelse med opbevaring af data

Fortrolige informationer skal altid være krypteret, når de opbevares på transportabelt udstyr, f.eks. tablets, mobiler, bærbare computere, m.m.

Brug af kryptering i forbindelse med dataudveksling

Det kræves, at e-mail og data, der indeholder fortrolige informationer, altid er krypteret under transmission.

Adgangskontrol og metoder

Adgangen til at udføre handlinger på kommunens IT-systemer beskyttes af autorisationssystemer. Systemerne har til formål at sikre mod uautoriserede ændringer, ordrer, fejl og svindel. Kommunens medarbejdere er medvirkende til beskyttelse af informationsaktiverne gennem korrekt brug af autorisationssystemerne.

Adgangskontrol til operativsystemer

Administration af arbejdsstationer

Generelt må administrative adgangskoder ikke gives til de arbejdsstationer, der anvendes i organisationen. Dispensation gives kun af sikkerhedsorganisationen.

Ændring af administrative kodeord

Administrative kodeord skal ændres hvert kvartal.
Administrative kodeord skal ændres hvis udenforstående får kendskab til disse, herunder administratorer der forlader kommunen.

Administratorbeskyttelse

Der skal benyttes systemadministrator-adgangskode på alle platforme.

Adgangskontrol for applikationer

Isolering af særligt kritiske brugersystemer

Særligt kritiske brugersystemer skal placeres på isoleret informationsbehandlingsudstyr.

Begrænset adgang til informationer

Adgang for brugere og hjælpepersonale til brugersystemers funktioner og informationer skal begrænses i overensstemmelse med de fastlagte forretningsbetingede krav.

Adgangsbegrænsning til informationer

Der bør implementeres adgangskontrol på systemer for at hindre uautoriseret adgang til data og funktionalitet. Detailopsætning og specificering afhænger af form og indhold af data, dokumenteret i risikovurderingen af systemet.

Logisk adgangskontrol

Retningslinier for kodeord

Ved brugeroprettelse eller nulstilling af kodeord skal brugere tildeles en sikker, midlertidig adgangskode, som skal ændres umiddelbart efter første anvendelse.

IT-Helpdesk skal etablere og vedligeholde en procedure for, hvordan en brugers identitet fastlægges, før en ny midlertidig adgangskode må udleveres.

Midlertidige kodeord skal være unikke, må ikke genbruges og opfylde de almindelige krav til kodeord.

Krav til længde af kodeord

Kodeord skal være mindst 8 tegn langt.

Krav til indhold af kodeord

Kodeord skal indeholde kombinationer fra mindst tre af følgende kategorier: Store bogstaver, små bogstaver, tal og specialtegn.

Der må ikke benyttes brugernavn, navn eller personlige datoer som en del af kodeord.

Krav til skift af kodeord

Kodeord skal skiftes efter højst 90 dage. Brugeren bliver adviseret 5 dage før udløb. Såfremt kodeord ikke bliver skiftet, bliver brugeren spærret.

Administration af adgangskontrol

Udvidede adgangsrettigheder

Rettigheder styres ved hjælp af processkemaer, der godkendes af leder eller dertil udpeget medarbejder.

De udvidede adgangsrettigheder må kun tildeles i begrænset omfang og alene ud fra et arbejdsbetinget behov.

De udvidede adgangsrettigheder skal registreres.

De udvidede adgangsrettigheder må ikke sættes i kraft, før den fornødne autorisation er indhentet.

Automatiserede systemtekniske processer skal anvendes i videst muligt omfang for at begrænse behovet for tildeling af udvidede rettigheder.

De enkelte brugerprogrammer skal, så vidt muligt, tilrettelægges, så de begrænser behovet for indgreb med udvidede rettigheder.

Der skal benyttes særlige brugeridentiteter til de udvidede rettigheder af hensyn til overvågning og opfølgning.

Registrering af brugere

Brugere skal have unikt brugernavn og bruger-id.

Systemejer skal autorisere brugeradgang og fører kontrol af, hvorvidt de ønskede adgangsrettigheder stemmer overens med de forretningsmæssigt behov.

Der skal ske en verifikation af at rettighedsniveauet er i overensstemmelse med kommunens generelle sikkerhedsretningslinjer.

Brugere kan se sine rettigheder via AD-search.

Serviceleverandører skal anvende tilsvarende eller samme autorisationsprocedure som kommunen.

Systemejer har ansvaret for at vedligeholde brugerfortegnelser for systemet, herunder hvordan brugere eller brugeres rettigheder fjernes eller ændres ved ophør eller ændring af brugeres jobfunktion.

Dokumentationen gemmes i kommunens ESDH-system.

Kontrol af, hvorvidt de ønskede adgangsrettigheder eventuelt krænker krav om funktionsadskillelse.

Retningslinier for adgangsstyring

Systemejere har det overordnede ansvar for at etablere og vedligeholde proceduren for adgangsstyring i hvert system. Dokumentationen gemmes i kommunens ESDH-system.

Identifikation af brugerprofiler for eksterne brugere

Eksterne brugerprofiler skal gennem konsistent navngivning være tydeligt angivet for at adskille disse fra fastansatte medarbejdere.

Standardkodeord og bruger-id'er må ikke anvendes på kommunens systemer. Disse skal ændres eller slettes.

Gennemgang af jobprofilroller

Alle jobprofilroller skal gennemgås mindst en gang årligt for at identificere inaktive profiler eller tilsvarende, der skal fjernes eller ændres.

Skift af administrator kodeord ved fratrædelse

Hvis en person med kendskab til administrative kodeord fratræder skal disse kodeord ændres med det samme af IT-Drift.

Medarbejderes omplacering

Ved ændringer af roller fjernes alle tidligere tildelte rettigheder for medarbejderne – via processkema.

Fratrædelse

Når ansættelse eller midlertidige kontrakter ophæves, skal alle tilknyttede rettigheder trækkes tilbage via processkema. Id-kort og lignende skal afleveres, og IT-udstyr skal inddrages inden sidste løn udbetales.

Brugerprofiler for konsulenter

Konsulenter tildeles som udgangspunkt ikke adgang til IT-systemerne. Begrænset adgang kan tildeles efter godkendelse fra systemejer eller dertil udpeget medarbejder. Der vil ske løbende opfølgning på eksterne brugere.

Brugerens ansvar

Valg af sikre kodeord

Det er brugerens ansvar at vælge tilstrækkeligt sikre kodeord i adgangskontrolsystemerne.

Adgangskontrol til netværk

Styring af netværksadgang

IT-Afdelingen skal ved styring af brugernes netværksadgang sikre imod uautoriseret anvendelse af fælles netværk og hertil knyttede tjenester.

Retningslinier for brug af netværkstjenester

Brugere skal kun have adgang til de tjenester, de er autoriseret til at benytte.

Autentificering ved adgang til netværket

Adgangen til det interne netværk fra andre lokationer end kommunens skal benytte kodeord.

Styring af systemadgang

Rapportering af sikkerhedshændelser

Adgangskoder til væsentlige systemer må aldrig lagres elektronisk i klartekst.

Automatiske afbrydelser

Systemer, f.eks. Citrix, hvor der ikke har været aktivitet i et fastlagt tidsrum, skal automatisk logge af.

Brug af systemværktøjer

IT-Drift skal begrænse og styre adgangen til systemværktøjer, fx utilities der kan påvirke eller omgå systemers eller enheders sikkerhed.
IT-Afdelingen skal definere, hvem der er autoriseret til at anvende hvilke systemværktøjer.
Dokumentationen findes i TopDesk.
Hvor funktionsadskillelse er påkrævet, må brugere ikke have adgang til både systemværktøjer og brugersystemer.

Identifikation og autentifikation af brugere

Alle brugere skal have en unik identitet til personlig brug.
Der skal benyttes en passende autentifikationsteknik til verifikation af brugernes identitet.

Brugeridentiteten skal kunne spores til den person, som er ansvarlig for en given aktivitet.

Sikker log-on

Systemadgang skal beskyttes af en sikker log-on-procedure.

Tildeling af brugerrettigheder

Systermejer bestemmer nødvendige brugerrettigheder for systemet. Dokumentationen for styring findes i kommunens ESDH-system og dokumentationen for tildeling findes i TopDesk.

Udvikling, anskaffelse og vedligeholdelse

Indkøb, udvikling og implementering af nye systemer i kommunen skal foregå kontrolleret for at undgå en unødvendig forøgelse af risiko for informationssikkerheden. Når løsninger implementeres bør sikkerhedsovervejelser altid indgå som en integreret del af processen. Alle indkøb af IT-systemer skal gennemgås af IT-Visitationen.

Anskaffelsesprocedurer

Det skal sikres, at nyanskaffelser ikke giver anledning til konflikt med eksisterende krav i sikkerhedsreglerne og arkitekturprincipperne.
Anskaffelser må ikke give anledning til forøget risiko for sikkerhedshændelser, med mindre at ledelsen accepterer den øgede risiko.
Ethvert nyt system skal gennemgå en risikovurdering. Det er systemejers ansvar at foretage denne.
Risikovurderingen skal dokumenteres i kommunens ESDH-system.
Anskaffelse og installation af nye systemer skal gennemgås af IT-Visitationen.

Sikkerhedskrav ved anskaffelser

Sikkerhedskrav til systemer

Kommunens ønsker til nye såvel som bestående systemer skal indeholde krav til sikkerheden med udgangspunkt i en risikovurdering.

Specifikation af sikkerhedskrav

Såfremt en overordnet risikovurdering retfærdiggør aktiviteten, skal sikkerhedskrav dokumenteres i kommunens ESDH-system i forbindelse med enhver nyanskaffelse eller opgradering.

Anskaffelser

IT-Afdelingen skal tilse at kun kendt og sikkert udstyr eller software med et defineret formål må anskaffes og tages i drift.
Udstyr og software må kun indkøbes fra leverandører som IT-Afdelingen vurderer som seriøse og som må forventes ikke at krænke tredjeparts ophavsret.

Applikationers behandling af informationer

Validering af uddata

Systemejer skal i samarbejde med IT-Afdelingen, sikre at uddata fra kommunens systemer eller applikationer valideres med det formål at sikre, data så vidt muligt er korrekte.

Integritet af meddelelser

Systemejer skal i samarbejde med IT-Afdelingen sikre, at der foretages risikovurderinger af, hvorvidt meddelelsers integritet skal beskyttes samt den mest hensigtsmæssige metode til at implementere dette på.

Kontrol af intern databehandling

Systemejer skal i samarbejde med IT-Afdelingen, sikre en kontrol af datas korrekthed i kommunens systemer eller applikationer med det formål at afsløre, om data kan eller er blevet modificeret, enten på grund af systemfejl eller bevidste handlinger f.eks. vha. et logudtræk.

Validering af inddata

Der skal genereres log over de aktiviteter der sender data ind i systemet.

Sikkerhed ved ændringer

Ændringer i standardsystemer

Ændringer i eksternt leverede systemer skal begrænses til nødvendige ændringer, og sådanne ændringer skal styres og dokumenteres omhyggeligt. Leverandørens dokumentation skal journaliseres enten i kommunens ESDH-system eller dokumentationsdrev.

Gennemgang af systemer efter ændringer

Når driftsmiljøerne ændres skal kritiske forretningssystemer gennemgås og testes for at sikre, at det ikke har utilsigtede afledte virkninger på kommunens daglige drift.

Ændringsstyring

Ved ændringer skal der foregå en gennemgang af sikringsforanstaltninger og integritetskontroller for at sikre, at disse ikke forringes ved implementeringen.
Der skal indhentes en formel godkendelse af større ændringen før arbejdet med den går i gang.
Systemdokumentation skal opdateres ved hver ændring.
Forældet systemdokumentation skal arkiveres eller destrueres.
Der skal vedligeholdes en versionsstyring for alle systemændringer.
Der skal vedligeholdes et kontrolspor for alle ændringer.
Driftsdokumentation for brugerne skal holdes opdateret, således at de stadig er gældende efter ændringen.

Implementeringen af ændringen skal foretages på et aftalt tidspunkt så den ikke forstyrrer de involverede forretningsydelser.

Integritet for programmer og data

Databaseintegritet

Databasesikkerhed, integritetsstyring og datavalidering skal anvendes for at reducere muligheden for kompromittering af integriteten.

Styring af sikkerhedshændelser

Ansvar og forretningsgange for sikkerhedshændelser

Ledelsen skal placere ansvar for at fastlægge forretningsgange der sikrer en hurtig, effektiv og metodisk håndtering af sikkerhedsbrud. Informationen findes på Medarbejderportalen.

Opdagelse og rapportering af hændelser

Rapportering af programfejl

Brugere der observerer programfejl, skal rapportere dette hurtigst muligt via IT-Helpdesk.

Rapportering af sikkerhedshændelser

IT-Drift eller eventuelle outsourcing partnere skal rapportere om hændelser af betydning for sikkerheden. Mere konkret skal fortrolighed, dataintegritet og tilgængelighed af systemer rapporteres via hændelsesloggen på Medarbejderportalen.

Rapportering af formodede sikkerhedshændelser

Ved konstatering af brud eller formodede brud på IT-sikkerheden skal rapportering straks ske til databeskyttelsesrådgiveren og efterfølgende i hændelsesloggen på Medarbejderportalen.

Reaktion på sikkerhedsmæssige hændelser

Proces for reaktion på hændelser

Den sikkerhedsansvarlige har ansvar for at definere og koordinere en struktureret ledelsesproces der sikrer en passende reaktion på sikkerhedshændelser.
IT-Afdelingen skal definere telefonnumre, e-mailadresser og elektroniske formularer til indrapportering af sikkerhedshændelser.
IT-Afdelingen skal etablere og vedligeholde en procedure på Medarbejderportalen der sikrer et passende svar til personer som rapporterer en mulig sikkerhedshændelse.

Kontrol og opfølgning på sikkerhedsbrud

Brud på sikkerheden, uautoriseret adgang og forsøg på uautoriseret adgang til systemer, informationer og data skal registreres og anmeldes til Datatilsynet inden for 72 timer efter konstatering.

Opfølgning på hændelser

Vurdering af tidligere hændelser

Mindst en gang om året skal informationssikkerhedskoordinatoren fremlægge for ISU den forgangne periodes hændelser og på denne baggrund anbefale, hvorvidt IT-systemet eller procedure kan forbedres eller præciseres. Fx forslag om opdaterede regler eller procedurer eller opdateret risikovurdering.

Indsamling af beviser

Hvis et sikkerhedsbrud afstedkommer et retsligt efterspil uanset om sikkerhedsbruddet er foretaget af en person eller en virksomhed så skal der indsamles, opbevares og præsenteres et fyldestgørende bevismateriale.

At lære af sikkerhedsnedbrud

Systemejer skal i samarbejde med IT-Afdelingen dokumentere typer og omfanget af sikkerhedsbrud og efterfølgende evaluere sikkerhedsbruddet.

Information om sikkerhedshændelser

Kommunen skal på faktuel vis informere berørte parter internt og eksternt om eventuelle sikkerhedshændelser. IT- og Digitaliseringschefen skal godkende alle eksterne meddelelser.

Opfølgning på rapporterede sikkerhedshændelser

Informationssikkerhedskoordinatoren er ansvarlig for at opsamle statistik for rapporterede sikkerhedshændelser. IT- og Digitaliseringschefen har ansvaret for at vurdere eventuelle sanktioner ift. medarbejdere.

Beredskabsplanlægning og fortsat drift

Risikostyring og katastrofeplanlægning har til formål at mindske risikoen for og effekten af uforudsete hændelser. Nødplaner skal være med til at opretholde driften, således at skaderne for kommunen minimeres.

Beredskabsplaner

Afprøvning af beredskabsplaner skal indeholde:

En skrivebordstest af de forskellige scenarier.
Simuleringer (med henblik på at træne deltagerne i håndtering af deres roller efter episoden).
Teknisk reetablering (sikring af at tekniske systemer kan reetableres effektivt)
Test af leverandørens faciliteter og ydelser (sikre at eksterne ydelser og produkter lever op til betingelserne i kontrakten).
Test af total afprøvning (afprøve at kommunen, personalet, udstyret, faciliteterne og nødprocedurerne kan håndtere katastrofer)

Afprøvning og vedligeholdelse af beredskabsplaner

Beredskabsplaner skal løbende afprøves og opdateres for at sikre, at de er tidssvarende og effektive. Test og efterfølgende evaluering skal dokumenteres i kommunens ESDH-system.

Ramme for beredskabsplaner

Beredskabet skal fastlægge en ensartet ramme for kommunens beredskabsplaner for at sikre, at alle planerne er sammenhængende og tilgodeser alle sikkerhedskrav, samt at de fastlægger prioriteringen af afprøvning og vedligeholdelse.

Uddannelse i beredskabsplaner

IT-Afdelingen har ansvaret for at der foregår tilstrækkelig uddannelse af medarbejdere i de aftalte beredskabsprocedurer relateret til IT, inklusive krisehåndtering.

Beredskabsstyringsproces

IT-Afdelingen skal udarbejde og vedligeholde en beredskabsstyringsproces, som skal behandle de krav til informationssikkerhed, der er nødvendige for kommunens fortsatte drift.

Iværksættelse af nødplaner

Det skal være klart defineret i beredskabsplanen, hvem der har ansvaret for at aktivere nødplaner.

Evakuering af medarbejdere

Evakuering signaleres med sirene eller ved personlig rømning i situationer, hvor sirenen ikke kan benyttes. Alle medarbejdere skal gå ud af nærmeste udgang og hen til udpeget samlingspunkt jf. evakueringsinstruksen og afvente yderligere informationer.

Aktivering af beredskabsplanen

Det skal være klart defineret, hvem der har ansvaret for aktivering af beredskabsplaner.
Medarbejdere, der udgør en del af beredskabsplaner, skal være informeret om dette ansvar.
Alle medarbejdere skal være informeret om beredskabsplanernes eksistens. Det er nærmeste leders ansvar at sikre, at medarbejderne er informeret om dette.

Beredskabsplan

Beredskabsplaner skal udarbejdes, afprøves og vedligeholdes for systemer og processer, som er kritiske for kommunens virksomhed.

Planlægning af beredskab

Opdatering af beredskabsplaner

Mindst 1 gang om året skal beredskabsplaner gennemgås med henblik på opdatering. Den daglige sikkerhedsansvarlige har ansvaret for denne gennemgang.

Ansvar for kritiske funktioner og processer

Nødprocedurer for kritiske processer

Der skal for alle forretningskritiske processer eksistere en opdateret nødprocedure, der kan sættes i drift.

Identifikation af kritiske processer

Alle forretningskritiske funktioner og deres relaterede, processer, systemer og ejere skal være identificerede og dokumenterede i kommunens ESDH-system eller på krypteret USB-nøgler.

Retablering af forretningskritiske systemer på ny lokation

For alle forretningskritiske systemer skal der forefindes en plan for reetablering på ny lokation.

Sikkerhedskopiering

Katastrofeplaner for backup

Hvert forretningskritisk system skal have en nødplan for at sikre data. Dette skal testes løbende.

Opbevaring af sikkerhedskopier på ekstern lokation

Datamedier til reetablering af forretningskritiske systemer skal opbevares uden for kommunens lokaliteter.

Nødplaner for sikkerhedskopiering

Alle forretningskritiske systemer skal have en nødplan for sikkerhedskopiering, således at risikoen for tab af data minimeres.

Lovgivning, kontrakter og etik

Mange aspekter af kommunens virke kan være omfattet af lovgivning. Det er nødvendigt at kommunen overholder gældende lovgivning, og foretager indrapportering som foreskrevet til offentlige myndigheder.

Overholdelse af lovmæssige krav

Lovbestemte data

Kommunen skal beskytte lovbestemte data mod ændring, sletning, samt uautoriseret adgang.

Overholdelse af lovgivningen
Ledelsen skal forlods sikre, at kommunen overholder gældende lovgivning.

Sikring af kommunens lovbestemte data
Kommunens lovbestemte data skal opbevares og behandles således at datatab, uautoriseret modifikation og forfalskning undgås.

Identifikation af relevant lovgivning
Ledelsen er ansvarlig for at alle eksterne sikkerhedskrav og kommunens håndtering heraf, klarlægges, dokumenteres og løbende vedligeholdes.

Ophavsret

Retningslinier for ophavsrettigheder
Ledelsen har det overordnede ansvar for at kommunen fastholder en passende opmærksomhed ikke at krænke tredjeparts ophavsrettigheder.
IT-Afdelingen skal vedligeholde dokumentation for ejendomsretten af licenser, originalmateriale og manualer. Dokumentationen findes i kommunens ESDH-system.
IT-Afdelingen skal løbende kontrollere at software-licensaftaler overholdes, fx at eventuelle begrænsninger i antal brugere, servere eller kopier overholdes.
Brugere må ikke kopiere, konvertere eller udtrække information fra billed- og lydfiler eller tilsvarende ressourcer med mindre dette specifikt tillades fra rettighedshaveren.
Brugere må ikke kopiere bøger, artikler, rapporter eller andre dokumenter, helt eller delvist, med mindre dette specifikt tillades fra rettighedshaveren.

Administration af softwarelicenser
Registrering af software licenser sker gennem IT-Afdelingens værktøj til licensstyring. Det er IT- og Digitaliseringschefens overordnede ansvar at der er et tilstrækkeligt antal licenser.
Afdelingerne skal koordinere brug af software-licenser med IT-Afdelingen.
Medarbejdere må ikke forpligte kommunen ved at acceptere licensvilkår i software, som er ikke er accepteret af IT-Afdelingen.

Identificerede love og regelsæt

Regulering på kryptografiområdet
Ansvaret for overholdelse af regulativer og brug af kryptografiske produkter påhviler systemejer for de systemer hvor disse implementeres.

Opbevaring og behandling af personoplysninger
Der må ikke behandles personoplysninger af fortrolig karakter på privat pc.

Databeskyttelsesloven gælder ved enhver opbevaring og behandling af persondata.

Beskyttelse mod misbrug

Misbrugsbeskyttelse af IT-udstyr

Anvendelse af IT-udstyr til uautoriserede formål må ikke finde sted.

Kontrol og revision

Beskyttelse af revisionsværktøjer

Adgangen til revisionsværktøjer skal begrænses for at forhindre misbrug.

Sikkerhed i forbindelse med revision

Revisionskrav og revisionshandlinger i forbindelse med systemer i drift skal planlægges omhyggeligt og aftales med de involverede for at minimere risikoen for forstyrrelser af kommunens forretningsaktiviteter.
De planlagte revisionshandlinger må kun omfatte læseadgang til systemer og data. Rettigheder tildeles via processkema.
Hvis revisionen nødvendiggør mere end læseadgang, må dette kun tillades på kopier af de berørte filer der skal slettes efter brug.
Al adgang i forbindelse med revision skal logges.
De personer, der udfører revisionen, skal være uafhængige af det reviderede område.

Sporbarhed

Behandling af personrelaterede informationer skal logges automatisk, således at det er muligt for en revisor at kontrollere hvem, der har arbejdet med hvilke informationer på hvilke tidspunkter.

Kontrol af overholdelse Databeskyttelsesloven

Databeskyttelsesrådgiveren skal kontrollere overholdelse af databeskyttelsesloven.

Revision af sikkerhedspolitik

Den eksterne revision skal kontrollere at sikkerhedspolitikken er indarbejdet i organisationen og overholdes. Kontrollen skal foretages mindst en gang årligt.

Sikkerhedstest af interne IT-systemer

Mindst en gang om året skal IT-Drift udføre uddybende sikkerhedstest af sikkerhedsniveauet i internt netværksudstyr og servere.