Middelfart Kommune

Informationssikkerhedsregler

4.1

22-08-2019

Indholdsfortegnelse

5 Informationssikkerhedspolitikker

5.1 Retningslinjer for styring af informationssikkerhed

5.1.1 Politikker for informationssikkerhed

Offentliggørelse af sikkerhedspolitik
Den overordnede informationssikkerhedspolitik, Organisering og styring af informationssikkerhed og Informationssikkerhedsregler (også kaldet Informationssikkerhedsbeskrivelsen), skal gøres bekendt for alle relevante interessenter, herunder alle medarbejdere der oprettes på Middelfart Kommunes IT-platform. Informationssikkerhedsreglerne og let tilgængelige informationer opdelt i temaer lægges på intranettet. Det er ledernes opgave at informere nye medarbejdere.

5.1.2 Gennemgang af politikker for informationssikkerhed

Revision af sikkerhedspolitik
Der skal ske revision af sikkerhedspolitikken mindst en gang om året.

Vedligeholdelse af sikkerhedspolitik
Organisering og styring af informationssikkerhed og Informationssikkerhedsregler, procedurer og tilhørende dokumentation skal vedligeholdes af Informationssikkerhedsgruppen.

Godkendelse af sikkerhedspolitik
Den overordnede informationssikerhedspolitik og Organisering og styring af informationssikkerhed skal godkendes af Middelfart Byråd.

Opfølgning på implementering af sikkerhedspolitikken
Hver enkelt leder skal løbende sikre, at Informationssikkerhedsbeskrivelsen bliver overholdt inden for eget ansvarsområde. Lederne skal endvidere sikre, at Informationssikkerhedsbeskrivelsen er dækkende inden for eget område.

6 Organisering af informationssikkerhed

6.1 Intern organisering

6.1.1 Roller og ansvarsområder for informationssikkerhed

Persondata-ansvarlig
Lederne er ansvarlige indenfor eget område med henblik på overholdelse af reglerne i Databeskyttelseforordningen og Databeskyttelsesloven.

Ejerskab
Der skal udpeges systemansvarlige og systemejere på alle relevante IT-systemer.

Sikkerhedsansvar for IT-funktioner
Informationssikkerhedsgruppen udarbejder og vedligeholder en liste over samtlige IT-systemer. Listen skal angive systemansvarlig og systemejer for hvert enkelt system.
Listen er publiseret og opdateret på Middelfart Kommunes Intranet.

Ansvar for adgangsrettigheder

Systemansvarlig skal fastlægge og løbende revurdere adgangsrettigheder i overensstemmelse med Databeskyttelsesforordningen og Databeskyttelsesloven.
Brugere må kun have adgang til det, man har brug for i sit daglige arbejde.
Det kan i praksis ske igennem de halvårlige autorisationskontroller.

Administration af internet-domænenavne

Der skal forefindes en liste over Middelfart Kommunes registrerede domænenavne, status for brug, betalingsoplysninger og dato for fornyelse. Staben har ansvaret for at denne liste forefindes.

Sikkerhedsorganisation

Informationssikkerhedsgruppen skal arbejde på at sikre at Informationssikkerhedsreglerne er synlige, koordinerede og i overensstemmelse med Den overordnede informationssikkerhedspolitik og Organisering og styring af informationssikkerhed.

Koordination af IT-sikkerheden

Koordination af sikkerheden på tværs i organisationen varetages af Øverste sikkerhedsansvarlige med bistand fra Informationssikkerhedsgruppen.

Ledelsens rolle

Lederne skal sikre, at Middelfart Kommunes informationssikkerhedspolitik, Organisering og styring af informationsikkerhed og Informationssikkerhedsregler (også kaldet informationssikkerhedsbeskrivelsen) overholdes ved at udlægge klare retningslinier, udvise synligt engagement samt sikre en præcis placering af ansvar.

Konsekvensvurdering

Ved konkrete hændelser mod IT-systemer vurderes konsekvenser af IT-afdelingen.

Overordnet risikovurdering

Øverste sikkerhedsansvarlige skal sikre, at der er udført en overordnet risikovurdering af trusselbilledet for Middelfart Kommune. Udfra en risikomatrix med værdierne 1-5 for henholdsvis sandsynlighed og konsekvens, bliver der løbende vurderet på mulige hændelser, hvis samlede værdi overstiger 6. Det er Øverste sikkerhedsansvarlige ansvar at igangsætte initiativer på baggrund af sårbarhedsanalysen.
Der skal være udført en overordnet risikovurdering, der indeholder konsekvensvurdering og sårbarhedsvurdering.
Risikovurderingen skal opdateres mindst en gang om året.
Risikovurderingen skal omfatte alle forretningskritiske IT-systemer.

6.1.2 Funktionsadskillelse

Sikring af forretningskritiske systemer

Forretningskritiske systemer skal beskyttes ved hjælp af funktionsadskillelse, således at risikoen for misbrug minimeres.

Adgang til produktionsdata

Systemadministratorers adgang til fortrolige oplysninger skal begrænses, registreres gennem logning. Stikprøvekontrol kan udføres.

6.1.3 Kontakt med myndigheder

Kontakt med myndigheder
Kontakt med andre myndigheder skal foregå på sikker vis.

6.1.4 Kontakt med særlige interessegrupper

Kontakt med særlige interessegrupper
Kontakt med særlige interessegrupper (leverandører, erfagrupper, tværkommunale fora mv.) skal foregå på sikker vis, såfremt der udveksles fortrolige oplysninger eller personoplysninger.

6.1.5 Informationssikkerhed ved projektstyring

Udarbejdelse af business case
Systemansvarlig er ansvarlig for at sikre informationssikkerheden i projektet. Det gøres ved i samarbejde med Staben/IT-afdelingen at udarbejde en business case, hvor IT-sikkerhedsaspekter er belyst.

6.2 Mobilt udstyr og fjernarbejdspladser

6.2.1 Politik for mobilt udstyr

Ejere af data på mobile enheder
Alle data på mobile enheder tilhører Middelfart Kommune.
Såfremt medarbejdere installerer eller opbevarer private data eller programmer på enhederne, forbeholder Middelfart Kommune sig retten til enhver tid at slette disse.

Adgang til bærbare computere
Bærbare pc'er skal beskyttes med kodeord. Ingen brugere må tildeles tidsubegrænset administratoradgang. IT-chefen kan tildele tidsubegrænsede administratorrettigheder, hvis der er særlig begrundelse herfor.

6.2.2 Fjernarbejdspladser

Adgang fra distancearbejdspladser
Adgang gives kun for brugere, der er autentificerede med brugernavn og kodeord samt enten en personlig digital nøgle eller en fysisk token.
Der skal anvendes krypteret forbindelse.

7 Personalesikkerhed

7.1 Før ansættelsen

7.1.2 Ansættelsesvilkår og -betingelser

Samarbejdsaftaler
For at sikre at Middelfart Kommunes informationssikkerhedsbeskrivelse ikke kompromitteres skal ethvert formaliseret eksternt samarbejde være baseret på en tidsbegrænset samarbejdsaftale.

Fortrolighedserklæring for tredjepart
En tredjepart, der får adgang til Middelfart Kommunes data, og som ønsker at anvende disse data eksternt, skal være omfattet af en fortrolighedserklæring samt databehandleraftale.

Information til eksterne partnere
Relevante interessenter skal informeres om krav til efterlevelse af Informationssikkerhedsbeskrivelsen i Middelfart Kommune.

Sikkerhed ved samarbejde med partnere
Ved integration af Middelfart Kommunes systemer og processer med tredjepart skal sikkerhedsrisici altid vurderes og dokumenteres af kommunens systemejer. Det kan i praksis gøres ved godkendelse af businesscase.

Sikkerhedsvurdering af tredjepart
I forbindelse med udarbejdelse af business case er der lavet en sikkerhedsvurdering af tredje part. Det kan evt. ske ved ekstern IT-revisions rapport eller lignende dokumentation.

7.2 Under ansættelsen

7.2.1 Ledelsesansvar

Det er ledelsens ansvar at alle medarbejdere:
Er tilstrækkeligt informeret om deres roller og ansvar i forbindelse med sikkerhed, før de tildeles adgang til Middelfart Kommunes systemer og data.
Er gjort bekendt med nødvendige retningslinier, således at de kan leve op til Middelfart Kommunes informationssikkerhedsbeskrivelse.
Opnår et opmærksomhedsniveau i spørgsmål vedrørende informationssikkerhed, der er i overensstemmelse med deres roller og ansvar i Middelfart Kommune.

7.2.2 Bevidsthed om, uddannelse og træning i informationssikkerhed

Uddannelse i informationssikkerhed
Alle medarbejdere skal læse og have tilstrækkelig kendskab til Middelfart Kommunes Overordnede informationssikkerhedspolitik, Organisering og styring om informationssikkerhed og Informationssikkerhedsregler (også kaldet informationssikkerhedsbeskrivelsen). Der bliver udbudt kurser i informationssikkerhed.

7.2.3 Sanktioner

Overtrædelse af sikkerhedsretningslinierne
Det er ledelsens ansvar at sanktioner for brud på Middelfart Kommunes politikker, regler eller retningslinier håndhæves konsekvent og i overensstemmelse med gældende lovgivning.

7.3 Ansættelsesforholdets ophør eller ændring

7.3.1 Ansættelsesforholdets ophør eller ændring

Fortrolighedserklæring ved fratrædelse
Ved fratrædelse skal der gøres opmærksom på gældende fortrolighedsaftaler.

Tavshedspligt forpligtigelse
Alle medarbejdere bliver ved ansættelsestidspunktet, i ansættelsesbrev, gjort opmærksom på forpligtigelse vedr. tavshedspligt.

Fratrædelse
Når ansættelse eller midlertidige kontrakter ophæves, skal alle tilknyttede rettigheder trækkes tilbage. Id-kort og lignende skal afleveres, og it-udstyr skal inddrages senest sidste arbejdsdag. Afgangskema skal fremsendes til IT-afdelingen, og medarbejdere skal slettes i fagsystemer.

8 Styring af aktiver

8.1 Ansvar for aktiver

8.1.1 Fortegnelse over aktiver

Lederne er ansvarlige for aktiver (fysisk udstyr, data eller indkøbte systemer) indenfor eget område.

8.1.2 Ejerskab af aktiver

Ejerskab af aktiver
Ejerskabet ligger i den afdeling som har indkøbt det pågældende IT-udstyr, IT-system m.v..
Alle data der produceres i Middelfart Kommune, tilhører Middelfart Kommune.

8.1.3 Accepteret brug af aktiver

Overvågning af sociale netværk
Som led i den almindelige netværksovervågning kan netværkstrafik til sociale netværk blive overvåget.

Middelfart Kommunes informationer på sociale netværk
Middelfart Kommunes fortrolige oplysninger og følsomme personoplysninger må ikke deles på sociale netværk.

8.1.4 Tilbagelevering af aktiver

Ejer skal tilbagelevere aktiver
Lederen er ansvarlig for tilbagelevering af udleveret IT-udstyr m.v. i forbindelse med medarbejderes ophør af ansættelsesforhold.

8.2 Klassifikation af information

8.2.1 Klassifikation af information

Informationer og data skal klassificeres som følger:
- Personoplysninger: Enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede). Ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator.
- Forretningskritisk: Data er forretningskritiske og bør sikres. Systemansvarlig vurderer om systemet er forretningskritisk.
- Andet: Information og/eller data er ikke en personoplysning eller forretningskritisk data.

For specifikke fagsystemer såsom eDoc kan data og informationer yderligere klassificeres som nedenfor:
- Offentligt: Materiale der frit må udleveres til offentligheden. Klassificeres som postliste / ikke-postliste.
- Fortroligt: Materiale der er tilgængeligt for en begrænset gruppe personer. Et eksempel kunne være bestemt afdeling (borgersag - staben) eller en en bestemt funktion fx arbejdsmiljøsag eller HR-sag.

- Internt brug: Materiale der er tilgængeligt for alle internt i organisationen.

8.2.2 Mærkning af information

Ansvar for klassifikation
Systemansvarlig skal sørge for, at data inden for eget område er klassificeret, som defineret i 8.2.1.

8.2.3 Håndtering af aktiver

Fortrolige data på mobile enheder
Det er IT-afdelingen, der afgør på hvilke enheder, der må ligge fortrolige oplysninger/følsomme personoplysninger.
IT-afdelingen afgør til enhver tid, hvilke mobile enheder og fabrikater der understøttes.
Der må KUN anvendes enheder ejet af Middelfart Kommune, altså INGEN anvendelse af private enheder (BYOD).
Såfremt der skal dispenseres for ovenstående, kræves det, at en løsning på andet teknisk udstyr, som minimum er på samme it-sikkerhedsniveau som Xenmobile Secure Apps. Dispensation gives af IT-chefen.

Udlevering af fortrolige informationer og oplysninger
Fortrolige informationer og personoplysninger må kun udleveres, hvis der foreligger underskrevet fortrolighedsaftale samt databehandleraftale, og der iøvrigt er hjemmel hertil i særlovgivning.
Personoplysninger og fortrolige oplysninger må kun udleveres til bemyndigede personer.

Procedurer for informationsudveksling
Systemansvarlig skal sikre, at der foreligger retningslinier og procedurer for udveksling af både fysisk og elektronisk information.

Udveksling af data
Når der udveksles personoplysninger, skal der anvendes sikre medier eller transmissionsprotokoller.
Eksempelvis må Skype, Facetime og Hangout ikke anvendes som videokonference-medie ifbm personoplysninger. Samme gør sig gældende ifht Dropbox, Google Drive, OneDrive, Icloud og lign. services.
IT-chefen kan til enhver tid afgøre hvorvidt ovennævnte medier har opnået et sikkerhedsniveau, der gør om mediet kan anvendes.

Udskrivning
Printere som benyttes til udskrivning af fortrolige informationer skal placeres i lokaler der ikke generelt er offentlig tilgængelige.

8.3 Mediehåndtering

8.3.1 Styring af bærbare medier

Opbevaring og registrering af datamedier
Systemansvarlig skal sikre at medierne eller informationerne på mediet klassificeres, og at brugere er instrueret i at opbevare mediet i henhold til regler for klassifikationen.

Brug af datamedier
Benyttelse af bærbare datamedier skal være begrundet i opgaveløsningen og dens karakter.

Beskyttelse af systemdokumentation

IT-afdelingen skal opbevare systemdokumentation sikkert.

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.

Virusscanning af mobile datamedier

Inden ibrugtagning skal brugeren scanne ethvert datamedie for virus, hvis det har været i brug på eksternt udstyr. Med datamedie menes for eksempel transportable hukommelsesenheder, transportable drev, cd'er, dvd'er, og disketter.

Brug af bærbare medier til fortrolige data

Når fortrolige informationer opbevares eller transporteres på bærbare medier, f.eks. USB-hukommelse, PDA'er, cd'er, dvd'er eller disketter, skal disse medier være krypterede.

8.3.2 Bortskaffelse af medier

Afskaffelse og genbrug af medier

Alle datamedier, for eksempel harddiske, disketter, cd, dvd, bånd og hukommelsesenheder, skal sikkerhedsslettes eller destrueres inden bortskaffelse.
IT-afdelingen vælger destruktionsmetode for de enkelte datamedier.

8.3.3 Fysiske medier under transport

Brug af mobile enheder

Bærbart udstyr skal medbringes som håndbagage under rejser.

9 Adgangsstyring

9.1 Krav til adgangsstyring

9.1.1 Politik for adgangsstyring

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.

9.1.2 Adgang til netværk og netværkstjenester

Overvågning af netværk

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

Overvågning af internet-brug

Middelfart Kommune har mulighed for at filtrere og begrænse internetadgang.

Styring af netværksadgang

IT-afdelingen skal sikre at brugernes netværksadgang sker i overensstemmelse med netværkets fælles adgangsretningslinier og øvrige krav. Formålet er at undgå 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.

Forbindelse til fremmede trådløse netværk
Brugere må forbinde sig til fremmede trådløse netværk, såfremt antivirus er installeret og opdateret. Systemer der indeholder fortrolige og/eller personoplysninger må kun tilgås på fremmede netværk via Citrix web interface.

Adgang til trådløse netværk
Brugere skal autentificeres ved hjælp af et certifikat før der gives adgang til Middelfart Kommunes trådløse netværk.

Gæsters brug af Middelfart Kommunes trådløse netværk
Netværket kan og må kun anvendes til internet-adgang, ikke til direkte adgang til interne systemer.
Gæster får adgang til gæstenettet ved hjælp af kodeord.

9.2 Administration af brugeradgang

9.2.1 Brugerregistrering og -afmelding

Der skal foreligge tilgangsskema for alle nye brugerkonti før en bruger kan oprettes.
Lederen er ansvarlig for at der afleveres afgangsskema når en medarbejder fratræder sin stilling.
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.

9.2.2 Tildeling af brugeradgang

Systemansvarlig skal sikre, at der kun autoriseres personer, der er beskæftiget med de formål, hvortil oplysningerne behandles.
De enkelte brugere må kun autoriseres til anvendelser, som de har behov for i deres daglige arbejde.
Der må endvidere autoriseres personer, for hvem adgang til oplysninger er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.

9.2.3 Styring af priviligerede adgangsrettigheder

Ændring af administrative kodeord
Administrative kodeord skal ændres hvis udenforstående får kendskab til disse, herunder administratorer der forlader Middelfart Kommune.

Administrator beskyttelse
Der skal benyttes systemadministrator kodeord på alle platforme.

9.2.4 Styring af hemmelig autentifikationsinformation om brugere

Styring af brugernavn og kodeord
Tildeling af brugernavn og kodeord og ændring af disse, må kun kunne udføres af systemadministrator.
Overdragelse af kodeord

Kodeord må ikke overdrages på ukrypterede forbindelser, for eksempel e-mail.

9.2.5 Gennemgang af brugeradgangsrettigheder

Halvårlige kontroller af autorisationer m.v.
Systemansvarlig skal halvårligt sikre at der foretages kontrol af autorisationer, afviste adgangsforsøg og låste brugere.
Kontrollerne skal dokumenteres i ESDH-systemet under systemets IT-sikkerheds sag.

9.2.6 Inddragelse eller justering af adgangsrettigheder

Inddragelse af privilegier ved fratrædelse
I forbindelse med fratræden eller afskedigelse af personale, er det nærmeste leder, der har ansvar for inddragelse af privilegier (f.eks. diverse udlånt it-udstyr, systemadgange mv).

Brugernedlæggelse ved aftrædelse
Det er den enkelte leders ansvar at informere IT-afdelingen og systemansvarlig, når en medarbejder fratræder sin stilling.
Systemansvarlig skal sikre at den pågældende bruger nedlægges i det enkelte IT- system.
IT-afdelingen er ansvarlig for sletning af data, herunder mail, kalender, p-drev, mobileenheder, pcer mv.
Den enkelte leder er ansvarlig for sletning og oprydning efter den fratrådte medarbejder på afdelingens fællesdrev.

Brugerprofiler for konsulenter
Begrænset adgang kan tildeles efter godkendelse fra den systemansvarlige.

9.3 Brugernes ansvar

9.3.1 Brug af hemmelig autentifikationsinformation

Brug af autologin funktioner
Automatisk login eller systemer hvor kodeord gemmes i genveje eller på funktionstaster må ikke benyttes i første sikkerhedsniveau.

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.

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

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 datoer som en del af kodeord.

Krav til skift af kodeord
Kodeord skal skiftes efter højst 90 dage.

9.4 Styring af system- og applikationsadgang

9.4.1 Begrænset adgang til informationer

Tildeling af rettigheder
Den systemansvarlige skal sikre sig, at der kun tildeles rettigheder til det brugeren har brug for for at kunne udføre sit daglige arbejde.

9.4.2 Procedurer for sikker log-on

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

9.4.3 System for administration af adgangskoder

Administration af rettigheder og adgangskoder
Kun systemadministratorer må administrere rettigheder og adgangskoder.

9.4.4 Brug af priviligerede systemprogrammer

Brug af systemværktøjer
IT-afdelingen skal begrænse og styre adgangen til systemværktøjer, der kan påvirke eller omgå systemers eller enheders sikkerhed.
IT-afdelingen skal sikre at unødige systemværktøjer ikke er installeret eller tilgængelige på brugeres pc'er.
IT-afdelingen skal sikre at brugen af systemværktøjer begrænses til et minimum af betroede og autoriserede brugere.
IT-afdelingen skal definere, hvem der er autoriseret til at anvende hvilke systemværktøjer.
Hvor funktionsadskillelse er påkrævet, må brugere ikke have adgang til både systemværktøjer og brugersystemer.

10 Kryptografi

10.1 Kryptografiske kontroller

10.1.1 Politik for anvendelse af kryptografi

Dokumentation af nøgler
Hvis der anvendes kryptografi skal krypteringsnøgle dokumenteres og arkiveres i kommunens ESDH-system.

10.1.2 Administration af nøgler

Administration af nøgler
Systemansvarlig er ansvarlig for administration og dokumentation af krypteringsnøgler.

11 Fysisk sikring og miljøsikring

11.1 Sikre områder

11.1.1 Fysisk perimetersikring

Indbrudsalarmer
Middelfart Kommune skal anvende tilstrækkelige alarmsystemer på relevante bygninger og lokaler.

Optageudstyr i sikre områder
Uautoriseret optageudstyr er ikke tilladt i sikre områder.

11.1.2 Fysisk adgangskontrol

Brug af adgangskontrolsystemer
Der skal anvendes adgangskontrolsystemer på relevante bygninger og lokaler.
Brug af personlige adgangskort
Medarbejdere skal benytte adgangskort / nøgle ved adgang udenfor normal arbejdstid.
Adgangskort / nøgler er personlige, skal opbevares forsvarligt, og må ikke overlades til andre.

11.1.3 Sikring af kontorer, lokaler og faciliteter

Adgang til kontorlokaler mv.
Borgere, leverandører m.v. må ikke have uhindret og uovervåget adgang til administrative kontorlokaler og faciliteter, hvori der foretages sagsbehandling.

11.1.4 Beskyttelse mod eksterne og miljømæssige trusler

Miljømæssig sikring af serverrum
Serverrum, krydsfelter og tilsvarende områder skal på forsvarlig vis sikres mod hændelser som brand, vand, eksplosion, varme og tilsvarende påvirkninger.

Brandsikring
Passende brandsikringsudstyr skal forefindes, og være korrekt placeret.

11.1.5 Arbejde i sikre områder

Aflåsning af lokaler og bygninger
Alle døre og vinduer med adgang til/fra bygningerne skal lukkes og låses ved arbejdstids ophør.

Døre til sikrede lokationer i bygningerne skal ligeledes aflåses.

Sikring af kontorer, lokaler og udstyr
Afdelinger, kontorer og andre lokaler, hvor der opbevares systemer med fortrolige og/eller følsomme personoplysninger, skal kunne låses. Der skal desuden benyttes et adgangskontrolsystem til styring af adgangen til lokalerne.

Ansvar for den fysiske adgangskontrol
Plan & Byg har ansvaret for administration af den fysiske adgangskontrol til kontorer og serverrum.

11.1.6 Områder til af- og pålæsning

Områder til af- og pålæsning er perimetersikret på Middelfart Rådhus. Al varemodtagelse til rådhuset sker ved henvendelse til Betjentstuen. Der er ikke adgang til sikrede områder for uautoriseret personel.

11.2 Udstyr

11.2.1 Placering og beskyttelse af udstyr

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

Distribueret IT-udstyr
Alle krydsfelter, afdelings serverrum og lignende faciliteter med delt IT udstyr skal aflåses for at hindre uautoriseret adgang til disse.

Aflåsning af hovedkrydsfelter og lignende teknikrum
Alle krydsfelter og andre teknikrum skal være aflåste.

Adgang til serverrum og hovedkrydsfelter
Adgang til serverrum og hovedkrydsfelter tillades kun med sikkerhedsgodkendelse, eller ved overvåget adgang af medarbejdere fra IT-afdelingen.

Adgang for serviceleverandører
Serviceleverandører må kun få adgang til sikre områder når dette er påkrævet.

Udlån af adgangskort
Adgangskort må udlånes til håndværkere, teknikere og andre, såfremt der er lovlig adgang for disse. Borgerservice & Fritidsafdelingen forestår udlevering af adgangskort.

11.2.2 Understøttende forsyninger (forsyningssikkerhed)

Køling
Serverrum skal sikres med veldimensionerede køleanlæg.

Nødstrømsanlæg
Alle forretningskritiske systemer skal beskyttes med nødstrømsanlæg til at sikre hurtig og korrekt system-nedlukning i tilfælde af strømudfald.

Forsyningssikkerhed
IT-afdelingen har ansvaret for at alle forsyninger som elektricitet, køl og ventilation skal have den fornødne kapacitet, og løbende inspiceres for at forebygge uheld der kan have indflydelse på it-systemerne.
Data-og telekommunikationsforbindelser skal etableres via minimum to adgangsveje for forretningskritiske systemer.

11.2.3 Sikring af kabler

Sikring af kabler
Kabler til datakommunikation skal beskyttes mod uautoriserede indgreb og skader.

Faste kabler og udstyr skal mærkes klart og entydigt.
Dokumentation skal opdateres når den faste kabelføring ændres.

11.2.4 Vedligeholdelse af udstyr

Vedligeholdelse af udstyr og anlæg
It-afdelingen skal vedligeholde udstyr efter leverandørens anvisninger.
Kun godkendte leverandører må udføre reparationer og vedligeholdelse.
Kritiske/følsomme informationer skal slettes fra udstyr der repareres eller vedligeholdes uden for Middelfart Kommune.

11.2.5 Fjernelse af aktiver

Fjernelse af udstyr fra Middelfart Kommune
Udstyr der indeholder fortrolige data, må kun fjernes efter behørig destruktion af data.
Udlån af udstyr skal være tidsbegrænset.

11.2.6 Sikring af udstyr og aktiver uden for organisationen

Fortrolige informationer i offentlige rum
Fortrolige informationer må ikke efterlades uden opsyn i offentlig tilgængelige rum.
Der skal udvises forsigtighed ved omtale af fortrolige informationer i offentlige rum.

11.2.7 Sikker bortskaffelse eller genbrug af udstyr

Afskaffelse eller genbrug af udstyr
Når udstyr bortskaffes eller genbruges skal kritiske/følsomme informationer og licensbelagte systemer fjernes, overskrives eller destrueres.

11.2.8 Brugerudstyr uden opsyn

Placering af udstyr
Udstyr skal placeres eller beskyttes så risikoen for skader og uautoriseret adgang minimeres. Udstyr skal placeres, så information ikke er tilgængelig for uvedkommende.

Tyverimærkning af IT-udstyr
Alt udstyr skal være tydeligt mærket for at minimere risikoen for tyveri.

11.2.9 Politik for ryddeligt skrivebord og blank skærm

Brug af kodeordsbeskyttet pauseskærm
Alle skal aktivere kodeordsbeskyttet skærmlås når en arbejdsstation forlades. Kodeordsbeskyttet skærmlås aktiveres automatisk efter 15 minutter uden brug. Ved Middelfart Kommunes tandpleje er arbejdsstationer tilknyttet tandbehandling fritaget fra førnævnte.

Opbevaring af fysiske dokumenter
Skriveborde skal ryddes for fortrolige dokumenter senest ved arbejdsdagens afslutning.

Opbevaring af fortrolige informationer på privat pc

Der må ikke opbevares personoplysninger eller fortrolige informationer på andet udstyr end Middelfart Kommunes servere.

12 Driftssikkerhed

12.1 Driftsprocedurer og ansvarsområder

12.1.1 Dokumenterede driftsprocedurer

Driftsafviklingsprocedurer
Driftsafviklingsprocedurer for væsentlige systemer skal være dokumenterede, ajourførte og tilgængelige for IT-afdelingen.

Driftsansvar
IT-afdelingen er ansvarlig for drift, administration og sikkerhed af egendriftede IT-systemer.

Dokumentation
IT-afdelingen skal løbende vurdere dokumentationsbehov for alle væsentlige systemer og IT-relaterede forretningsgange.

Adskillelse af udvikling, test og drift
Systemers udviklings- og testmiljøer skal være teknisk og/eller fysisk adskilt fra driftsmiljøet.

Sikring af serversystemer
Servere skal sikres og testes inden implementering i produktionsmiljøet.

Sikring af arbejdsstationer inden ibrugtagning
Alle PC'er, arbejdsstationer og lignende skal sikres af IT-afdelingen inden brug. Brugerne må ikke omgå denne sikring

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

Integration af informationssystemer
Hvis integration af informationssystemer resulterer i en forøget risiko, så skal denne vurderes og godkendes af IT-afdelingen.

Overvågning af tilgængelighed
IT-afdelingen skal løbende overvåge alle væsentlige IT-systemer.

12.1.2 Ændringsstyring

Ændringsstyring
Ved ændringer skal der foregå en gennemgang af sikringsforanstaltninger og integritetskontroller for at sikre, at disse ikke forringes ved implementeringen.
Implementeringen af ændringen skal foretages på et aftalt tidspunkt så den ikke forstyrrer de involverede forretningsydelser. Fortrinsvis skal ændringer implementeres uden for normal åbningstid.

12.1.3 Kapacitetsstyring

Kapacitetsplanlægning
IT-systemernes dimensionering skal afpasses efter kapacitetskrav. Belastning skal overvåges således at opgradering og tilpasning kan finde sted løbende.

12.1.4 Adskillelse af udviklings test- og driftsmiljøer

Forretningskritiske systemer
For forretningskritiske systemer skal test- og driftsmiljøer være funktionelt adskilte.

12.2 Beskyttelse mod malware

12.2.1 Kontroller mod malware

Antivirus produkter på arbejdsstationer
IT-afdelingen skal sikre, at der er installeret aktive anti-virus produkter på samtlige computere i Middelfart Kommune, og at disse opdateres højest et døgn efter leverandørens opdateringer.

Adware
Adware beskyttelse baseres på medarbejder-"awareness", sikkerhedsindstillinger i internetbrowser, begrænsninger i brugeres muligheder for softwareinstallation.

Spyware
Installation af spyware søges undgået gennem begrænsningerne i muligheder for softwareinstallation. Installation af spyware søges undgået gennem patch-management-processer.

Ansvar for bekæmpelse af malware
IT-afdelingen forestår bekæmpelse af virus, spyware og adware.

Antivirusprogrammer
Anti-virusprogrammer skal være installeret på bærbare computere og hjemmearbejdspladser. Softwaren skal holdes opdateret ved opgradering mindst en gang om ugen.

12.3 Backup

12.3.1 Backup af information

Overvågning af procedurer for sikkerhedskopiering
Muligheden for at retablere data fra backup systemer skal regelmæssigt testes.

Deaktivering af beskyttelsesmekanismer
Det er under ingen omstændigheder tilladt at deaktivere eller omgå Middelfart Kommunes beskyttelsesmekanismer, herunder anti-virus produkter.

Sikkerhedskopiering af data på serversystemer
IT-afdelingen sørger for opbevaring og sikkerhedskopiering af alle forretningskritiske informationer på serversystemer.

Sikkerhedskopiering af data på andre systemer

Såfremt forretningskritiske data ikke opbevares på serversystemer skal systemansvarlig være ansvarlig for etablering af relevant sikkerhedskopiering.

12.4 Logning og overvågning

12.4.1 Hændelseslogning

Halvårlige kontroller af autorisationer m.v.
Systemansvarlig skal sikre at der foretages kontrol af autorisationer, afviste adgangsforsøg og låste brugere halvårligt.

12.4.2 Beskyttelse af logoplysninger

Sikring af hændelsesloggen
Systemansvarlig er ansvarlig for at leverandøren sikrer hændelsesloggen i minimum 6 måneder.

12.4.3 Administrator- og operatørlog

Overvågning af serviceleverandøren
Systemansvarlig 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.

12.4.4 Tidssynkronisering

Tidssynkronisering af log
Systemansvarlig skal sikre at det enkelte system er tidssynkroniseret så loggen er tidsstemplet korrekt.

12.5 Styring af driftssoftware

12.5.1 Softwareinstallation på driftsystemer

Krav til indstillinger af internet-browser
MS Internet Explorer (i Citrix) og Google Chrome browser (i Citrix) er de eneste internetbrowser som kommunen tillader. Sikkerhedsindstillinger i Internt Explorer samt Chrome browser opsættes og redigeres af IT-afdelingen. Brugerne må ikke ændre denne opsætning. Kun IT-afdelingen kan dispensere herfor.

Installation af programmer på arbejdsstationer
Som udgangspunkt er det kun IT-afdelingen der må installere programmer på Middelfart Kommunes arbejdsstationer.
Operativsystemer og applikationer må kun installeres og ændres af IT-afdelingen på godkendt udstyr.
Kun IT-afdelingen kan dispensere herfor.

12.6 Sårbarhedsstyring

12.6.1 Styring af tekniske sårbarheder

Større operativsystemopdatinger, for eksempel "service packs".
Når større opdateringer, for eksempel "service packs", er gjort tilgængelige fra leverandører skal systemejer i samarbejde med IT-afdelingen vurdere om disse skal installeres.

Information om nye trusler, virus og sårbarheder
IT-afdelingen skal holde sig orienteret inden for de benyttede platforme.
Systemansvarlig skal, når nye sårbarheder annonceres, vurderer for relevans og alvorlighed. Hvis nødvendigt skal passende reaktion prioriteres for at mindske organisationens sårbarhed.

Styring af anti-virus
IT-afdelingen skal kunne styre anti-virus på alle systemer fra en central lokation. Med styring menes tvungen opdatering, scanning og oprydning.

Større programpakkeopdateringer, for eksempel "service packs".
Når større opdateringer, for eksempel service packs, er gjort tilgængelige fra leverandører skal IT-afdelingen vurdere om disse skal installeres.

Rettelser til applikations-programpakker
Systemejer skal i samarbejde med IT-afdelingen løbende vurdere tilgængelige sikkerhedsrettelser, for eksempel "patches" eller "hot-fixes", til anvendte programpakker. Udrulning/installation på relevante systemer skal foretages i henhold til gældende procedure efter vurdering og positiv funktions- og kompatibilitetstest.

Rettelser til operativsystemer
IT-afdelingen skal mindst hver uge vurdere tilgængelige sikkerhedsrettelser, for eksempel "patches" eller "hot-fixes", til anvendte operativsystemer. Udrulning/installation på relevante systemer skal foretages senest en uge efter vurdering og positiv funktions- og kompatibilitetstest.

Softwareopdateringer generelt
IT-afdelingen skal holde sig informeret om alle programrettelser til alle programmer, der anvendes i Middelfart Kommune og snarest installere disse på alle computere, f.eks. servere og arbejdsstationer, når det vurderes at rettelserne har positiv indflydelse på den samlede sikkerhed.
IT-afdelingen skal forestå installation af alle større programrettelser, når det vurderes, at disse har positiv indflydelse på den samlede sikkerhed.

Anti-virus-produkter på servere
Der skal være installeret anti-virus beskyttelse på alle systemer, hvor dette er muligt.

12.6.2 Begrænsninger på softwareinstallation

Administration af arbejdsstationer
Generelt må administrative adgangskoder ikke gives til de arbejdsstationer, der anvendes i organisationen. Dispensation gives kun af IT-afdelingen.

Sikkerhedsindstillinger i web-browser
Der må kun anvendes godkendte webbrowsere. Brugerne må ikke forsøge at omgå eller bryde sikringsforanstaltningerne.

Download af filer fra internet
Filer må downloades fra internet i begrænset arbejdsmæssigt omfang.

Download af programmer fra internet

Det er ikke tilladt at hente programmer fra internet, medmindre det er relateret til løsning af arbejdsopgaver.

Medarbejderes private brug af internetadgang

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

12.7 Overvejelser i forbindelse med audit af informationssystemer

12.7.1 Kontroller i forbindelse med audit af informationssystemer

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 Middelfart Kommunes forretningsaktiviteter.
De planlagte revisionshandlinger må kun omfatte læseadgang til systemer og data.
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.

13 Kommunikationssikkerhed

13.1 Styring af netværkssikkerhed

13.1.1 Netværksstyring

Personlige firewalls

Alle arbejdsstationer skal benytte firewalls.

Adgang til netværket

Netadgang og systemadgang begrænses ved brug af godkendte firewalls.

Adgang til applikationer på Middelfart Kommunes netværk

Der gives kun adgang til applikationer på internt netværk, som er sikkerhedsgodkendt af it-afdelingen.

PDA

IT-afdelingen afgør til enhver tid, hvilke mobile enheder og fabrikater der understøttes.
Der må KUN anvendes enheder ejet af Middelfart Kommune, altså INGEN anvendelse af private enheder (BYOD).

Installation af trådløst udstyr

Medarbejdere må ikke installere eller ibrugtage udstyr der giver trådløs netadgang, med mindre der specifikt er givet lov hertil fra it-afdelingen.

Placering af trådløse netværk

Trådløst udstyr må kun forbindes til den eksisterende infrastruktur ved hjælp af sikkerhedsgodkendt firewall. Det er udelukkende IT-afdelingen, som må opsætte sådant udstyr.

Brug af trådløse lokalnetværk

Brug af trådløse netværk tillades, såfremt personlig firewall er slået til, samtidig med at der anvendes Nfuse som adgang til kommunens applikationser og systemer.

Netværksdokumentation
IT-afdelingen skal vedligeholde et opdateret netværksdiagram.
Netværksdiagrammet skal omfatte samtlige netværksforbindelser.
Netværksdiagrammet skal omfatte samtlige trådløse netværk.
Netværksdokumentationen skal indeholde en beskrivelse af den logiske administration.

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

Sikring af netværk
IT-afdelingen skal sikre at Middelfart Kommunes netværk beskyttes.

Tilslutning af udstyr til netværk
Medarbejdere eller konsulenter må ikke koble udstyr (ikke ejet af Middelfart Kommune) sammen med det interne netværk. Kun it-afdelingen må koble udstyr på det interne netværk.

Installation af netværksudstyr
Det er ikke tilladt at installere netværksudstyr uden forudgående sikkerhedsgodkendelse.

Adgang til aktive netværksstik
Adgang til aktive netværksstik skal styres af IT-afdelingen.
Netværksadgang skal kontrolleres og styres af IT-afdelingen. Kun nødvendige adgange må være aktive i infrastrukturen. Alle øvrige skal være lukket ned.

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

Installation og brug af modem
Det er ikke tilladt at installere modem uden forudgående sikkerhedsgodkendelse.
IT-afdelingen skal godkende alle installationer af modem og tilsvarende udstyr til datakommunikation.

13.1.2 Sikring af netværkstjenester

Godkendelse af krypteringsprodukter
IT-afdelingen skal godkende alle produkter der indeholder kryptografi, før disse må benyttes til fortrolige data.

Afvikling af programmer i forbindelse med Internetsurfing
Det er tilladt at afvikle browserbaserede programmer, for eksempel netbank-programmer, forudsat sikkerhedspolitikken i øvrigt overholdes.

Trådløse netværk for gæster
Middelfart Kommune tilbyder trådløs netværkstjeneste til gæster.

Fjernstyring og administration
Værktøjer til fjernadministration såsom "KMD-skygge" eller Teamviewer tillades KUN i forbindelse med intern support.

13.1.3 Opdeling af netværk

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

13.2 Informationsoverførsel

13.2.1 Politikker og procedurer for informationsoverførsel

Brug af kryptering i forbindelse med dataudveksling
Det kræves, at e-mail og data, der indeholder personoplysninger eller fortrolige informationer, altid er krypteret under transmission.

13.2.2 Aftaler om informationsoverførsel

Databehandleraftale
Ved informationsoverførsler af personoplysninger eller fortrolig information skal der altid indgåes databehandleraftale med tredjepart.

13.2.3 Elektroniske meddelelser

Opbevaring og sletning af e-post
E-mail der indeholder personoplysninger, skal behandles i overensstemmelse
med Databeskyttelsesforordningen og Databeskyttelsesloven.
Al journalisering skal ske i eDoc eller fagsystemer. Når e-mails er journaliseret skal de straks slettes fra Outlook.

Fortrolig mail
E-mail med personoplysninger skal før ekstern afsendelse krypteres med godkendt software. På intranettet er anført udførlig beskrivelse af anvendelsen af hhv. sikker post, digital post samt Doc2mail.

Phishing og bedrageri
Uanset at Middelfart Kommune udfører indholdscanning af alle e-mails, skal brugere være opmærksomme på "phishing" og "social engineering". Der kan være tale om tilsyneladende oprigtige e-mails der forsøger at franarre personlige eller fortrolige oplysninger, eller forsøger at få brugeren til at foretage uønskede handlinger, såsom kryptering af filer.

Ejerskab
Middelfart Kommune betragter alle e-mails som Middelfart Kommunes ejendom. Ved konkret grund kan din Outlook profil blive overtaget af Øverste sikkerhedsansvarlige, din leder eller en af lederen udpeget kollega.

Vedhæftede filer
IT-afdelingen blokerer for følgende filtyper : *.exe, *.vbs, *.zip, *.scr, *.bat, *.cmd. IT-afdelingen udvider eller indskrænker mængden af blokerede filtyper løbende, baseret udfra en løbende sikkerhedsvurdering.

Sagsbehandling og journalisering af e-mail

Modtaget og afsendt e-mail skal journaliseres og behandles efter samme principper, som gælder for almindelig fysisk post og fax.

Automatisk videresendelse af email

Det er ikke tilladt, at opsætte agenter eller lignende, som automatisk videresender mail til eksterne mail-konti. Det er dog tilladt i forbindelse med ferie, sygdom, barsel mv. at opsætte agenter eller lignende som videresender indkomne mails til anden kollegas arbejdsmail (*@middelfart.dk).

Automatisk indholdsfiltrering

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

Spam-mail beskyttelse

IT-afdelingen bortfiltrerer e-mail der opfylder Middelfart Kommunes 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.

13.2.4 Fortroligheds- og hemmeligholdelsesaftaler

Indhold af fortrolighedserklæringerne

Fortrolighedserklæringen må kun anvendes når der ikke behandles personoplysninger.
En fortrolighedserklæring skal indeholde nedenstående punkter:

- Definition af de informationer der er omfattet.
- En fastlagt løbetid.
- Beskrivelse af hvad der skal ske når aftalen udløber.
- 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.

Aftaler om informationsudveksling

Ved udveksling af information og software imellem Middelfart Kommune og evt. tredje part skal der foreligge en skriftlig aftale.Ved behandling af personoplysninger, skal det fremgå af aftalen, at databehandler overholder Middelfart Kommunes informationssikkerhedspolitik, Organisering og styring af informationsikkerhed og Informationssikkerhedsregler (også kaldet informationssikkerhedsbeskrivelsen). Middelfart Kommunes skabelon for databehandleraftaler ligger til grund for udarbejdelsen af aftaler, som omhandler behandling af personoplysninger.

14 Anskaffelse, udvikling og vedligeholdelse af systemer

14.1 Sikkerhedskrav til informationssystemer

14.1.1 Analyse og specifikation af informationssikkerhedskrav

Anskaffelsesprocedurer

Det skal sikres, at nyanskaffelser ikke giver anledning til konflikt med eksisterende krav i sikkerhedspolitikken og at nyanskaffelser altid overholder de sikkerhedsmæssige krav som beskrevet i Databeskyttelsesforordningen.

Anskaffelse og installation af nyt informationsbehandlingsudstyr og -systemer skal godkendes af IT-afdelingen.

14.1.2 Sikring af applikationstjenester på offentlige netværk

Sikring af applikationer på offentlige netværk
Der skal benyttes sikre autentifikations- og autorisationsprocesser for at sikre service-transaktioner over offentlige netværk
Datas integritet og fortrolighed skal sikres, når der benyttes applikations-services over offentlige netværk
Eksempelvis:

- Integritetssikring (såsom hashing)
- Kryptografiske løsninger (såsom SSL, SFTP, HTTPS, sikre API'er eller webservices)

14.1.3 Beskyttelse af handelsapplikationer og -tjenester

Online transaktioner
Privacy skal sikres for alle parter involveret i transaktionen
Der skal anvendes industristandarder for signaturer (kryptografiske løsninger) af alle involverede parter i transaktionerne.

14.2 Sikkerhed i udviklings- og hjælpeprocesser

14.2.1 Sikker udviklingspolitik

Validering af inddata
Data, der sendes ind i systemerne, skal valideres for korrekthed.

14.2.2 Procedurer for styring af systemændringer

Ved ændringer skal der foregå en gennemgang af sikringsforanstaltninger og integritetskontroller for at sikre, at disse ikke forringes ved implementeringen.
Implementeringen af ændringen skal foretages på et aftalt tidspunkt så den ikke forstyrrer de involverede forretningsydelser. Fortrinsvis skal ændringer implementeres uden for normal åbningstid.

14.2.3 Teknisk gennemgang af applikationer efter ændring af driftsplatforme

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.

14.2.4 Begrænsning af ændringer af softwarepakker

Ændringer i standardsystemer
Ændringer i eksternt leverede systemer skal begrænses til nødvendige ændringer, og sådanne ændringer skal styres omhyggeligt.

14.2.5 Principper for udvikling af sikre systemer

Specifikation af sikkerhedskrav

Sikkerhedskrav skal være dokumenteret i forbindelse med enhver væsentlig IT-system-nyanskaffelse eller IT-systemopgradering. Dette gælder for kundetilpassede og standardsystemer. Dokumentationen skal fremgå af den udarbejdede businesscase.

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 professionelle og som må forventes ikke at krænke tredje parts ophavsret.

Kravspecifikation skal omhandle følgende områder:
- Adgangskontrol
- Alle væsentlige hændelser logges og overvåges.
- Tilstrækkelig datapålidelighed på udvalgte dele af udviklingsprocessen, og kontrol heraf.
- Tilstrækkelig datapålidelighed på alle dele af udviklingsprocessen, og kontrol heraf.
- Beskyttelse imod fortrolighedskrænkelser i det omfang systemet skal behandle fortrolige og/eller personoplysninger.
- Overholdelse af relevante love eller kontrakter.
- Mulighed for backup af data og system.
- Mulighed for genetablering efter kritiske, uforudsete fejlsituationer.
- Beskyttelse imod pålidelighedskrænkelser, for eksempel som følge af uautoriserede ændringer.
- Krav til viden og uddannelse af driftspersonale.

14.2.8 Systemsikkerhedstest

14.2.9 Systemgodkendelsestest

Godkendelse af nye eller ændrede systemer
Der skal udarbejdes business cases for alle nye systemer. Businesscase godkendes af Øverste sikkerhedsansvarlige. Øverste sikkehedsansvarlige kan delegere denne kompetence. Systemansvarlig og systemejer er i samarbejde med IT-afdelingen ansvarlige for godkendelse af nye versioner og opdateringer af eksisterende systemer.

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.

Ændringer i væsentlige systemer
Alle ændringer i væsentlige systemer udføres efter en procedure, der indeholder muligheden for reetablering.

14.3 Testdata

14.3.1 Sikring af testdata

Sikring af testdata
Testdata skal sikres på samme måde som produktionsdata.

15 Leverandørforhold

15.1 Informationssikkerhed i leverandørforhold

15.1.1 Informationssikkerhedspolitik for leverandørforhold

Ved kontraktindgåelse skal det sikres, at leverandøren overholder kommunens Overordnede informationssikkerhedspolitik, Organisering og styring af informationssikkerhed og Informationssikkerhedsreglerv (også kaldet informationsikkerhedsbeskrivelsen). Før kontraktindgåelse skal der udarbejdes og godkendes en business case. Hvis systemet behandler personoplysninger skal der tillige indgåes en databehandleraftale.

15.1.2 Håndtering af sikkerhed i leverandøraftaler

Det skal sikres, at kommunens informationssikkerhedsbeskrivelse overholdes. Dette sikres gennem business case, kontrakt, databehandleraftale samt indhentning af IT-revisionserklæringer.

15.1.3 Forsyningskæde for informations- og kommunikationsteknologi

Leverandøren skal kunne levere:
De nødvendige teknologiske muligheder for autentifikation, kryptering og overvågning.
De nødvendige tekniske opsætninger til at sikre opkoblinger i overensstemmelse med kontrakten.
Adgangskontrol der sikrer mod uvedkommendes adgang.

15.2 Styring af leverandørydelser

15.2.1 Overvågning og gennemgang af leverandørydelser

Systemansvarlig er ansvarlig for overvågning og gennemgang af leverandørydelser.

15.2.2 Styring af ændringer af leverandørydelser

Styring af ændringer hos leverandøren
Systemansvarlig skal sikre, at ændringsstyring af leverandørens ydelser ikke forringer IT-sikkerhed eller drift.

16 Styring af informationssikkerhedsbrud

16.1 Styring af informationssikkerhedsbrud og forbedringer

16.1.1 Ansvar og procedurer

Ansvar og forretningsgange for sikkerhedshændelser
Databeskyttelsesrådgiveren indsamler alle rapporterede sikkerhedhændelser jf. Databeskyttelsesforordningen og orientere i fornødent omfang Øverste sikkerhedsansvarlige.
Informationssikkerhedsgruppen skal behandle større sikkerhedshændelser.

Alle andre sikkerhedshændelser håndteres af IT-afdelingen.

Proces for reaktion på hændelser
IT-afdelingen skal sikre en passende reaktion på sikkerhedshændelser. Alle hændelser skal samles og videregives til det kommende IT-styregruppemøde.

Sikkerhedshændelser der vedrører personoplysninger, skal følge den beskrevne procedure for håndtering af brud på persondatasikkerheden.

16.1.2 Rapportering af informationssikkerhedshændelser

Rapportering af virus angreb
Ved mistanke om virus, skal det omgående rapporteres til IT-afdelingen.

16.1.3 Rapportering af informationssikkerhedssvagheder

Rapportering af programfejl
Ved programfejl skal pågældende systemejer kontaktes.

Rapportering af formodede sikkerhedshændelser
Ved konstatering af brud eller formodede brud på IT-sikringsforanstaltninger skal rapportering straks ske til IT-afdelingen. Rapportering kan ske telefonisk, via intranet (http://itfejlmelding) eller pr mail (IT-Support/Helpdesk).

Sikkerhedshændelser der vedrører personoplysninger, skal følge den beskrevne procedure for håndtering af brud på persondatasikkerheden.

16.1.4 Vurdering af og beslutning om informationssikkerhedshændelser

Vurdering af og forslag til aktion på en informationssikkerhedshændelse foretages enten
af Databeskyttelsesrådgiveren eller IT-afdelingen.
Øverste sikkerhedsansvarlige / IT-afdelingen tager endelig beslutning om aktion på en informationssikkerhedshændelse.
Ved større sikkerhedshændelser rådgiver Informationssikkerhedsgruppen.

16.1.5 Håndtering af informationssikkerhedsbrud

Et eventuelt informationssikkerhedsbrud skal håndteres af IT-afdelingen eller hvis det omhandler brud på persondatasikkerheden af Databeskyttelsesrådgiveren jf. den beskrevne procedure.

16.1.6 Erfaring fra informationssikkerhedsbrud

Erfaringer fra informationssikkerhedsbrud skal danne grundlag for gennemgang af den samlede informationssikkerhedsbeskrivelse.

16.1.7 Indsamling af beviser

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

18 Overensstemmelse

18.1 Overensstemmelse med lov- og kontraktkrav

18.1.1 Identifikation af gældende lovgivning og kontraktkrav

Identifikation af relevant lovgivning

Øverste sikkerhedsansvarlig skal sikre, at alle lovkrav, bekendtgørelser med videre, vedrørende IT-området, herunder datasikkerhed for behandling af personoplysninger, følges.
Status på efterlevelsen af love og regler inden for IT-området, herunder datasikkerhed for behandling af personoplysninger, skal monitoreres løbende og revideres mindst en gang hvert år.

Opbevaring og behandling af personoplysninger

Databeskyttelsesforordningen og Databeskyttelsesloven gælder ved enhver opbevaring og behandling af personoplysninger.
Der må ikke behandles personoplysninger af fortrolig karakter på privat pc og/eller privat mobilt udstyr.
Personoplysninger må ikke opbevares eller behandles på bærbar pc, medmindre kryptering anvendes og Databeskyttelsesforordningen og Databeskyttelsesloven overholdes, samt sikkerhedsforanstaltninger svarende til sikkerhedsbekendtgørelsen overholdes.

18.1.2 Immaterielle rettigheder

Retningslinier for ophavsrettigheder

Systemansvarlig skal sikre, at Middelfart Kommune ikke krænker tredje parts ophavsrettigheder.
Systemansvarlig skal vedligeholde dokumentation for ejendomsretten af licenser, originalmateriale og manualer.
Brugere må ikke installere systemer uden autoriserede licenser.
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.

Identifikation af relevante patenter

Systemansvarlig skal sikre at der i eksisterende og nyindkøbte IT-systemer identificeres relevante patenter.

Administration af softwarelicenser

Registrering af software licenser sker gennem IT-afdelingen. Det er IT-chefens overordnede ansvar, at der er et tilstrækkeligt antal licenser.

18.1.3 Beskyttelse af registreringer

Elektroniske dokumenter

Elektroniske kopier af dokumenter, for eksempel indscannede dokumenter og faxer, med personoplysninger må kun behandles på Middelfart Kommunes IT-udstyr.

Opbevaring og bortskaffelse af data

Kortholderdata må kun opbevares i det tidsrum, som er nødvendigt i henhold til gældende lovgivning og forretningsmæssige formål.
Der skal foreligge en procedure for håndtering af opbevaringstiden for data.
Data må kun opbevares i det tidsrum, som er nødvendigt.

Lagring og adgangsrettigheder til systemdokumentation

Systemdokumentation opbevares i mindst 5 år.

Lovregulerede data
Middelfart kommune skal beskytte lovregulerede data mod ændring, sletning, samt uautoriseret adgang.

Sikring af virksomhedens lovbestemte data
Middelfart kommune lovbestemte data skal opbevares og behandles således at datatab, uautoriseret modifikation og forfalskning undgås.

18.1.4 Privatlivets fred og beskyttelse af personoplysninger

Principper for behandling af personoplysninger
Middelfart kommune skal sikre at personoplysninger behandles loyalt, lovligt og på en gennemsigtig måde for den registrerede
Middelfart kommune må indsamle personoplysninger til udtrykkeligt angivne og legitime formål.
Personoplysninger skal være relevante, tilstrækkelige og må kun bruges til det fastsatte formål.
Personoplysninger skal være korrekte og ajour og det skal sikres at urigtige oplysninger omgående kan rettes eller slettes.
Personoplysninger må ikke opbevares længere end nødvendigt.
Middelfart kommune skal sikre korrekt behandling og dokumentere at databeskyttelsesforordningen overholdes.

Lovlig behandling af personoplysninger
Behandling af personoplysninger må kun ske hvis den registrerede har givet sit samtykke, eller:
Behandling er nødvendig af hensyn til opfyldelsen af en kontrakt, som den registrerede er part i, eller af hensyn til gennemførelsen af foranstaltninger, der træffes på dennes anmodning forud for indgåelsen af en sådan kontrakt.
Behandlingen er nødvendig for at overholde en retlig forpligtelse, som gælder for Middelfart kommune.
Behandlingen er nødvendig for at beskytte den registreredes vitale interesser.
Behandlingen er nødvendig for udførelse af en opgave i samfundets interesse eller henhørende under offentlig myndighedsudøvelse, som Middelfart kommune har fået pålagt.
Behandlingen er nødvendig og legitim, medmindre den registreredes interesser og rettigheder går forud herfor, navnlig hvis den registrerede er et barn. Dette gælder ikke for den behandling, som offentlige myndigheder foretager som led i udførelsen af deres opgaver.
Behandling af personoplysninger, der er nødvendig til historiske, statistiske eller videnskabelige forskningsformål, er lovlig dog med visse forbehold.

Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden
Middelfart kommune (den dataansvarlige) skal senest 72 timer efter et brud på persondatasikkerheden, foretage anmeldelse til Datatilsynet. Anmeldelsen skal begrundes, hvis den ikke er indgivet inden for 72 timer
Anmeldelse skal blandt andet beskrive bruddets art, karakteren af bruddet på persondatasikkerheden, konsekvenser og afhjælpende foranstaltninger.
Middelfart kommune skal dokumentere alle brud på persondatasikkerheden, herunder kendsgerningerne i forbindelse med bruddet, dets virkninger og de iværksatte afhjælpende foranstaltninger.

Databeskyttelsesrådgiver for personoplysninger
Databeskyttelsesrådgiver skal rådgive Middelfart Kommune i forhold til gennemførelsen af passende tekniske og organisatoriske foranstaltninger og procedurer, så behandlingen opfylder Databeskyttelsesforodningens krav og sikrer beskyttelsen af den registreredes rettigheder.

Enhver der udfører arbejde under kommunen og som får adgang til personoplysninger, må kun behandle disse efter instruks fra kommunen.

Forudgående godkendelse og høring for behandling af personoplysninger

Middelfart Kommune, eller databeskyttelsesrådgiver, skal foretage høring hos Datatilsynet inden behandlingen af personoplysninger, hvis konsekvensanalyse vedrørende databeskyttelse viser, at en behandling kan indebære store konkrete risici.
Datatilsynet kan vurdere, at det er nødvendigt at udføre en forudgående høring vedrørende en behandling, der sandsynligvis kan indebære specifikke risici for registreredes rettigheder og frihedsrettigheder i medfør af dens karakter, omfang eller formål.

Gennemsigtige oplysninger og meddelelser for personoplysninger

Middelfart Kommune (den dataansvarlige) skal sikre, at der er fastsat gennemsigtige og lettilgængelige regler for behandlingen af personoplysninger og udøvelsen af registreredes rettigheder.
Middelfart Kommune skal sikre, at det er muligt at kunne udlevere alle oplysninger og meddelelser vedrørende behandlingen til den registrerede i en letforståelig form og i et klart og forståeligt sprog, som er tilpasset den registrerede

Databeskyttelse af personoplysninger

Middelfart Kommune skal iværksætte passende tekniske og organisatoriske foranstaltninger og procedurer, så behandlingen opfylder databeskyttelsesforordningens krav og sikrer beskyttelsen af den registreredes rettigheder.
Middelfart Kommune skal gennemføre mekanismer med henblik på at sikre, at kun de personoplysninger, der er nødvendige til det specifikke formål med behandlingen, behandles
Middelfart Kommune skal sikre at oplysninger ikke indsamles eller opbevares ud over, hvad der er nødvendigt til disse formål, både med hensyn til mængden af oplysninger og opbevaringsperioden.
Middelfart Kommune skal med sikringsmekanismerne særligt sikre, at personoplysninger ikke stilles til rådighed for et ubegrænset antal personer.

Ret til at klage over behandling af personoplysninger

De registrerede har ret til at klage til tilsynsmyndigheden, hvis de finder, at behandlingen af deres personoplysninger ikke er i overensstemmelse med databeskyttelsesforordningen og gældende dansk lovgivining om databeskyttelse.

Ret til indsigt i personoplysninger

Den registrerede har til enhver tid ret til, at anmode Middelfart Kommune om at få indsigt i, hvilke personoplysninger der behandles om vedkommende.
Hvis sådanne personoplysninger behandles, skal Middelfart Kommune blandt andet fremlægge formål, kategorier, modtagere, tidsrum for behandling og klagemulighed.

Princip for videregivelse af personoplysninger

Enhver videregivelse af de personoplysninger, som Middelfart Kommune behandler må kun finde sted, hvis betingelserne i databeskyttelsesforordningen overholdes.

Konsekvensanalyse vedrørende databeskyttelse for personoplysninger

Middelfart Kommune (den dataansvarlige) skal gennemføre systematisk konsekvensanalyse for beskyttelse af personoplysninger, hvis behandlingen af personoplysninger kan indebære specifikke risici for registreredes rettigheder og frihedsrettigheder.

Analysen skal omfatte beskrivelse af den planlagte behandling, en analyse af risiciene for registreredes rettigheder og de sikkerhedsforanstaltninger der er nødvendige for at opfylde databeskyttelsesforordningen.

Videregivelse af personoplysninger ved anvendelse af bindende virksomhedsregler
Datatilsynet står for godkendelse af bindende virksomhedsregler, såfremt de er retligt bindende, gælder for og anvendes af Middelfart Kommune og omfatter alle kommunens medarbejdere.

Videregivelse af personoplysninger
Middelfart Kommune må kun overføre personoplysninger til et tredjeland eller en international organisation, hvis der er indført de fornødne garantier i et retligt bindende instrument, der sikrer beskyttelsen af personoplysninger
Hvis aftale om videregivelse af personoplysninger er baseret på standardbestemmelser om databeskyttelse eller bindende virksomhedsregler, jf. databeskyttelsesforordningen, kræves ikke yderligere godkendelse.
Videregivelse af oplysninger baseret på standardbestemmelser kræver ikke yderligere godkendelse hos Datatilsynet.
Videregivelse af oplysninger baseret på kontraktbestemmelser, kræves forudgående godkendelse hos Datatilsynet.
Middelfart Kommune skal sikre forhåndsgodkendelse hos tilsynsmyndighed, hvis de fornødne garantier for beskyttelsen af personoplysninger ikke er omhandlet i et retligt bindende instrument.

Ret til berigtigelse af personoplysninger
Den registrerede kan kræve, at Middelfart Kommune retter forkerte personoplysninger om den registrerede.
Den registrerede har ret til at få rettet ufuldstændige personoplysninger, bl.a. ved at kræve en berigtigelse.

Udpegning af en databeskyttelsesrådgiver for personoplysninger
Middelfart Kommune skal udpege en databeskyttelsesrådgiver.
Middelfart Kommune kan udpege den databeskyttelsesrådgiver på grundlag af dennes faglige kvalifikationer, ekspertise på området for databeskyttel-seslovgivning og -praksis samt evne til at udføre opgaver vedrørende personoplysninger.
Middelfart Kommune skal sikre, at databeskyttelsesrådgiverens øvrige arbejdsopgaver er forenelige med den pågældendes opgaver og ansvar som databeskyttelsesrådgiver og ikke medfører interessekonflikt.
En databeskyttelsesrådgiver udpeges for en periode på mindst to år.
En databeskyttelsesrådgiver kan være ansat af Middelfart Kommune eller udføre sit hverv på grundlag af en tjenesteydelseskontrakt.
Middelfart Kommune skal meddele navnet på og kontaktoplysningerne for databeskyttelsesrådgiveren til Datatilsynet og offentligheden.

18.1.5 Regulering af kryptografi

Regulering på kryptografiområdet
Middelfart Kommune skal efterleve nationale regler for kryptering. Dette gælder også for medarbejdere, der besøger andre lande, medbringende bærbart og mobilt udstyr. Juridisk afdeling og den sikkerhedsansvarlige er ansvarlige for at informere medarbejdere om de regler og retningslinier, der er gældende.
Ansvaret for overholdelse af regulativer og brug af kryptografiske produkter påhviler systemansvarlig for de systemer, hvorpå disse implementeres.

18.2 Gennemgang af informationssikkerhed

18.2.1 Uafhængig gennemgang af informationssikkerhed

Revision af informationssikkerhedsbeskrivelsen

Den overordnede informationsikkerhedspolitik og Organisering og styring af informationssikkerhed gennemgåes og revideres mindst en gang årligt.

Informationssikkerhedsreglerne gennemgåes og revideres efter behov inden for rammerne af den overordnede informationssikkerhedspolitik og Organisering og styring af informationssikkerhed.

Uafhængig audit af informationssikkerheden
Middelfart Kommunes ISMS (Ledelsessystem for informationssikkerhed) skal være underlagt en, for IT-afdelingen, uafhængig audit.
Audit skal omfatte:

- Informationssikkerhedspolitik og Organisering og styring af informationssikkerhed
- Informationssikkerhedsregler - og disses efterlevelse
- IT-sikkerhedsprocedurer
- ISMS processer

Audit skal gennemføres 1 gang om året, eller hvis der sker væsentlige ændringer i kommunens ISMS.

Overvågning og audit af outsourcingleverandør
Middelfart Kommune kan foretage audit af leverandøren, alternativt kan intern auditrapport, IT-revisionsrapport, årlig risikovurdering eller IT-outsourcing-erklæring indgå i overvågningen.
Middelfart Kommune overvågning og audit skal fastslå, om leverandøren har passende organisering og ansvarsfordeling, og om de eksisterende kontroller følges og er tilstrækkelige
Periodiske service-statusmøder skal omhandle sikkerhedsrelaterede emner såsom sikkerhedshændelser og resultater af KPI'er.

18.2.2 Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder

18.2.3 Undersøgelse af teknisk overensstemmelse

Sikkerhedstest af interne IT-systemer
Der bliver årligt udført en penetrationstest, fra yderside af firewall og ind, af eksternt sikkerhedsfirma.
Der bliver, på baggrund af denne test, genereret en sikkerhedsrapport, der påpeger eventuelle sikkerhedssvagheder.
Rapport inddrages i beslutningsprocessen for styrkelse af sikkerhedsniveauet i Middelfart Kommune