Lemvig Kommune

Regler ISO 27002:2013

2.0

03-01-2019

Lemvig Kommune

Indholdsfortegnelse

5 Sikkerhedspolitikker

IT-sikkerhedspolitikken skaber grundlaget for et passende og tilstrækkelig højt IT-sikkerhedsniveau i Lemvig Kommune, som sikrer fortrolighed, dataintegritet og tilgængelighed. Dette er en vigtig forudsætning for effektivitet og kvalitet i kommunens serviceydelser.

5.1 Retningslinjer for styring af IT-sikkerhed

5.1.1 Politikker for IT-sikkerhed

Offentliggørelse af IT-sikkerhedspolitik
IT-sikkerhedspolitikken skal offentliggøres og kommunikeres til alle relevante interessenter, herunder alle medarbejdere.

Sprog for IT-sikkerhedspolitik
IT-sikkerhedspolitikken skal kun eksistere på det sprog, der er hovedsproget i organisationen.

Omfang af IT-sikkerhedspolitik
IT-sikkerhed defineres som de samlede foranstaltninger til at sikre fortrolighed, tilgængelighed og integritet. Foranstaltninger inkluderer tekniske, proceduremæssige, lov- og regelmæssige kontroller.

Godkendelse af IT-sikkerhedspolitik
IT-sikkerhedspolitikken skal godkendes af Kommunalbestyrelsen.

5.1.2 Gennemgang af politikker for IT-sikkerhed

Ansvar for vedligeholdelse af IT-sikkerhedspolitikken
IT-sikkerhedspolitikken skal vedligeholdes af Chefen for Digitalisering & IT.

Revision af IT-sikkerhedspolitik
Der skal ske revision af IT-sikkerhedspolitikken mindst hvert tredje år.

6 Organisering af IT-sikkerhed

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 IT-sikkerheden.

6.1 Intern organisering

6.1.1 Roller og ansvarsområder for IT-sikkerhed

Koordination af IT-sikkerheden
Ansvaret for koordination af IT-sikkerhedstiltag varetages af Direktionen. Digitaliseringsstyregruppen støtter Direktionen med anbefalinger vedrørende IT-sikkerhed.

IT-sikkerhedsorganisation
Direktionen har ansvaret for at sikre, at strategien for IT-sikkerhed er synlig, koordineret og i overensstemmelse med kommunens mål.

Direktionens rolle
Direktionen skal støtte kommunens IT-sikkerhed ved at udlægge klare retningslinier, udvise synligt engagement samt sikre en præcis placering af ansvar.

Forsikring mod hændelser
Direktionen skal vurdere, om forsikring kan medvirke til minimering af risiko for tab. Især på områder, hvor sikringsforanstaltninger er vurderet som uhensigtsmæssige eller utilstrækkelige, skal dette overvejes.

Krav til ejerskab
Alle IT-systemer, der er risikovurderet, skal have udpeget en ejer.

Sikkerhedsansvar for IT-funktioner
Alle kritiske IT-funktioner der kræver specialviden, færdighed eller erfaring skal identificeres, og der skal udpeges en driftsansvarlig for hvert system.

Sikkerhedsansvar for IT-systemer
Chefen for Digitalisering & IT har ansvar for vedligeholdelse af en liste over samtlige IT-systemer. Listen angiver henholdsvis den sikkerhedsansvarlige dataejer og systemejer af hvert enkelt system.

Ansvar for adgangsrettigheder
Systemets ejer har ansvaret for at fastlægge og løbende revurdere adgangsrettigheder i overensstemmelse med kommunens IT-sikkerhedspolitik. Se afsnit 9.2 Administration af brugeradgang.

Administration af internet-domænenavne
Ansvaret for registrering af domænenavne ligger hos Chefen for Digitalisering & IT.

Persondataansvarlig
Som øverst persondataansvarlig er udpeget Chefen for Direktionssekretariatet. Hver direktørområde skal udpege en persondataansvarlig.
Den persondataansvarlige skal

- Vejlede ledere, brugere og serviceleverandører om deres ansvar og gældende procedurer i forhold til reglerne på vedr. behandling af persondata.
- Indenfor sin organisatoriske enhed sikre, at der er foretaget anmeldelse af alle anmeldelsespligtige behandlinger til Datatilsynet.
- Have overblik over hvilke personoplysninger, der behandles indenfor den pågældende organisatoriske enhed.

Digitalisering & IT har ansvaret for kommunens fortegnelser over behandling af persondata. De persondataansvarlige på de enkelte direktørområder sørger sammen med Digitalisering & IT for at holde fortegnelserne opdateret.

6.1.2 Funktionsadskillelse

Sikring af forretningskritiske systemer
Systemer, der er risikovurderet til at være forretningskritiske, skal beskyttes ved hjælp af funktionsadskillelse, således at risikoen for misbrug af privilegier minimeres.

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

Systemadministratorers adgang til fortrolige oplysninger skal begrænses.

Adskillelse af test/udvikling og drift
Testmiljøet skal være så identisk med driftsmiljøet som muligt.

6.1.3 Kontakt med myndigheder

Samarbejde med tilsynsmyndigheden for personoplysninger
Den øverste persondataansvarlige samarbejder efter anmodning med tilsynsmyndigheden ved udøvelsen af dennes hverv, navnlig ved at udlevere oplysninger.
Kommunen skal svare tilsynsmyndigheden inden for en rimelig frist, som fastsættes af tilsynsmyndigheden.
Svaret skal omfatte en redegørelse for de iværksatte foranstaltninger og de opnåede resultater som reaktion på bemærkningerne fra tilsynsmyndigheden.

6.1.4 Kontakt med særlige interessegrupper

Information om nye trusler, virus og sårbarheder
- Digitalisering & IT er ansvarlig for eksternt samarbejde med de fornødne informationskanaler, herunder samarbejde omkring IT-sikkerhed med relevante eksterne interessegrupper og sikkerhedsorganisationer.
- Digitalisering & IT skal holde sig orienteret inden for de benyttede platforme.
- Digitalisering & IT skal informere relevante personer i ledelsen om nye trusler, som potentielt kan berøre de pågældende forretningsenheder.
- Digitalisering & IT skal etablere en proces for identifikation af nye sårbarheder. Der skal udpeges en ansvarlig person eller gruppe for dette.

Når nye sårbarheder annonceres, skal de vurderes for relevans og alvorlighed. Hvis nødvendigt skal passende reaktion, f.eks. installation af sikkerhedsrettelser, prioriteres for at mindske organisationens sårbarhed.
Processen skal omfatte gennemgang og opdatering af konfigurationsstandarder, så det sikres, at der tages højde for nye sårbarhedsproblemer.

6.1.5 IT-sikkerhed ved projektstyring

Projektmodellen skal indeholde følgende overvejelser omkring IT-sikkerhed
- Kravspecifikationen skal indeholde kravene til IT-sikkerhed.
- Identifikation af nødvendige sikringstiltag skal blandt andet gøres ved hjælp af risikovurderinger.
- IT-sikkerhed bør være en integreret del af projektledelse.

6.2 Eksterne samarbejdspartnere

Information til eksterne partnere
Relevante interessenter skal informeres om krav til efterlevelse af IT-sikkerhedspolitikken i kommunen.

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

Aftaler om informationsudveksling

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

IT-sikkerhedsvurdering af tredjepart
Der skal udføres en IT-sikkerhedsvurdering af tredjepart før et eventuelt samarbejde.

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

IT-sikkerhed i forhold til borgere og andre
Før borgere og andre må få adgang til kommunens IT-systemer, skal alle IT-sikkerhedsforhold være afklaret.

6.3 Risikostyring

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

Overordnet risikovurdering
Der skal være udført en overordnet risikovurdering, der indeholder konsekvensvurdering og såbarhedsvurdering ultimo 2017. Risikovurderingen skal omfatte væsentlige IT-systemer og den skal opdateres mindst hvert andet år.

Risikoanalyse
Der skal udføres detaljeret risikoanalyse for de områder, hvor den overordnede risikovurdering begrunder det.

Konsekvensvurdering
Konsekvenser af hændelser imod IT-systmerne skal løbende vurderes af den ansvarlige leder for det enkelte område.
Den samlede konsekvensvurdering skal opdateres hvert andet år.

7 Personalesikkerhed

IT-sikkerheden i kommunen afhænger i høj grad af medarbejderne. De skal uddannes i IT-sikkerhed i relation til deres jobfunktion, og modtage nødvendige informationer. Endvidere er det nødvendigt med regler, der beskriver sikkerhedsforhold, når et ansættelsesforhold slutter.

7.1 Før ansættelsen

7.1.1 Screening

Baggrundscheck i form af dokumentation af ansatte
Den kompetenceansvarlige for ansættelse og afskedigelse skal tilse, at der i forhold til jobfunktionen sker et forsvarligt baggrundscheck af medarbejdere med adgang til IT-systemer.

Ren straffeattest
For regler om indhentelse af straffeattest henvises til personalepolitikken.

7.1.2 Ansættelsesvilkår og -betingelser

Aftale om ansættelse
Faste og midlertidige medarbejdere skal underskrive en aftale ved ansættelsen, der beskriver kommunens og medarbejderens ansvar og forpligtelser vedrørende IT-sikkerhed.

Tavshedspligtserklæring ved ansættelse
Alle medarbejdere skal underskrive en tavshedspligtserklæring ved ansættelsen. Denne kan være en del af ansættelseskontrakten. Der kræves ikke særskilte erklæringer for konsulenter, men det tilstræbes, at fortrolighed indgår i aftalegrundlaget. Praktikanter og andet ulønnet personale skal udfylde tavshedserklæring (blanket S-4923).

Indhold ved tavshedspligtserklæringer
- Definition af de informationer der er omfattet.
- Beskrivelse af hvad der skal ske, når aftalen udløber.
- Sanktioner ved brud på fortrolighedspligten.

Ansættelsesbrevet skal indeholde
Tavshedspligtsserklæring.

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 kommunens systemer og data.
- er gjort bekendt med nødvendige retningslinier, således at de kan leve op til kommunens IT-sikkerhedspolitik.
- er motiverede til at leve op til kommunens IT-sikkerhedspolitik og retningslinier.
- opnår et opmærksomhedsniveau i spørgsmål vedrørende IT-sikkerhed, der er i overensstemmelse med deres roller og ansvar i kommunen.

7.2.2 Bevidsthed, uddannelse og træning i informationssikkerhed

Uddannelse i sikkerhedspolitikken
Alle nye IT-brugere introduceres senest på første arbejdsdag for kommunens IT-sikkerhedspolitik. Alle IT-brugere skal desuden have træning i kommunens IT-sikkerhedspolitik og baggrundsviden omkring denne. Kommunalbestyrelsesmedlemmerne introduceres for kommunens IT-sikkerhedspolitik i starten af valgperioden. Ved udskiftning i løbet af valgperioden foretages individuel introduktion.
Det er direktøren/lederens ansvar at sikre introduktionen dette samt føre dokumentation herfor.

Sikkerhedsuddannelse for IT-medarbejdere
Alle IT-medarbejdere skal specifikt uddannes i sikkerhedsaspekter for at minimere risikoen for sikkerhedshændelser.
IT-medarbejdere skal løbende gennemgå produktspecifik sikkerhedsuddannelse, for de IT-produkter der er mest udbredte i kommunen.

Uddannelse i klassificering af informationer
Alle ansatte skal modtage instruktioner om, hvorledes data og dokumenter klassificeres (fortrolighed).

7.2.3 Sanktioner

Overtrædelse af IT-sikkerhedsretningslinierne
Det er ikke tilladt at omgå IT-sikkerhedsmekanismer. Det er ikke tilladt at foretage uautoriseret afprøvning af IT-sikkerheden. Bevidste eller gentagne overtrædelser kan medføre at ansættelses- eller samarbejdsforholdet overvejes fra kommunens side.
Hændelser, hvor medarbejdere er involverede, bliver håndteret konsekvent i overensstemmelse med gældende personalepolitik.
Det er ledelsens ansvar, at sanktioner for brud på kommunens politikker, regler eller retningslinier håndhæves konsekvent og i overensstemmelse med gældende lovgivning. Digitalisering & IT giver besked ved mistanke om overtrædelse.

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.

8 Styring af systemer, udstyr og data

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 jf. afsnit 8.2.

8.1 Ansvar for systemer, udstyr og data

8.1.1 Fortegnelse over systemer, udstyr og data

Registrering af IT-udstyr
Det er Digitalisering & ITs ansvar, at alt relevant IT-udstyr er registreret med ejer (afdeling/institution), bruger, serienummer og fakturaoplysninger. Digitalisering & IT opdaterer oversigt over relevant udstyr.

8.1.2 Ejerskab af systemer, udstyr og data

Ansvar og ejerskab for privat udstyr
Medarbejderen skal acceptere, at kommunen må slette data på privat udstyr, der anvendes til opbevaring af kommunens data.
Kommunen er ikke erstatningspligtig for tyveri, bortkomst, skade eller tab af personlige data for privat udstyr.
Medarbejderen har ansvar for tab af kommunens data på privat udstyr.

8.1.3 Accepteret brug af aktiver

Brug af mobile enheder

Bærbart udstyr skal medbringes som håndbagage under rejser.

8.1.4 Tilbagelevering af udstyr og data

Data på privat udstyr ved ansættelsens ophør
Medarbejderen skal slette kommunes data fra privat udstyr ved ansættelsens ophør.
Medarbejderen skal være indforstået med, at enheden kan nulstilles ved ansættelsens ophør, hvis arbejdsrelateret data har været opbevaret på enheden.

Returnering af aktiver ved fratrædelse
Ledelsen har ved en medarbejders fratrædelse ansvar for, at alle aktiver og rettigheder, som Lemvig Kommune har stillet til rådighed, returneres og slettes.

8.2 Klassifikation af data

8.2.1 Klassifikation af data

Data klassificeres som følgende
- Offentligt: Materiale der frit må udleveres til offentligheden.
- Fortroligt: Materiale der er tilgængeligt for en begrænset gruppe personer.
- Internt brug: Materiale der er tilgængeligt for alle internt i organisationen.
- Personhenførbart: Data er relateret til et individ, for eksempel en borger eller en medarbejder.

Ved klassificeringen skal der tages hensyn til gældende lovgivning.

8.2.2 Mærkning af data

Klassifikationsmærkning
Datamedier, som indeholder fortrolige personhenførbare data, skal mærkes "fortroligt".

8.2.3 Håndtering af systemer, udstyr og data

Kontrol med data kategorier
Chefen for Digitalisering & IT er ansvarlig for at definere egnede og relevante IT-sikkerhedskontroller til beskyttelse af de enkelte datakategorier. Hvis der er tale om kritiske data, skal der udarbejdes yderligere detaljerede kontroller ud fra en risikovurdering

Fortrolige data på mobile enheder
Der må opbevares fortrolige og personhenførbare data på mobile enheder, såfremt disse data beskyttes med et produkt, der er godkendt af Digitalisering & IT og overholder persondatalovens regler. Ved udlevering af mobileenheder så som i-Pads og mobiltelefoner, udleveres vejledning og regler omkring brugen af mobile enheder.

8.3 Håndtering af datamedier

Med datamedie menes for eksempel transportable hukommelsesenheder, transportable drev/harddiske, cder, dvder, disketter og usb-nøgler.

8.3.1 Styring af bærbare datamedier

Opbevaring og registrering af datamedier
Den enkelte leder skal sikre, at medarbejdere informeres om, at datamedierne eller data på mediet skal klassificeres, og at medarbejderne er instrueret i at opbevare datamediet i henhold til regler for klassifikationen.

Brug af datamedier
Benyttelse af bærbare datamedier skal være forretningsmæssigt begrundet.

Forretningsgangen for beskyttelse af datamediers indhold kan omfatte
- Håndtering og mærkning.
- Adgangsbegrænsning.
- Log over tildelte autorisationer.

Beskyttelse af følsomme og fortrolige data på datamedier
Digitalisering & IT skal etablere procedurer, der sikrer datamediers indhold mod uautoriseret adgang og misbrug af datamediernes indhold.

Virusscanning af mobile datamedier
Inden ibrugtagning skal brugeren scanne ethvert datamedie for virus, hvis det har været i brug på eksternt udstyr.

Beskyttelse af systemdokumentation
Digitalisering & IT skal opbevare systemdokumentation passende sikkert.
Adgangsrettigheder til systemdokumentation skal holdes på et minimum og godkendes af systemejer.

Brug af bærbare datamedier til fortrolige data
Manglende kryptering tillades hvis datamedierne, der benyttes til transport af fortrolige data, under transporten er overvåget af betroede personer.

9 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 data gennem korrekt brug af autorisationssystemerne.

9.1 De forretningsmæssige krav til adgangsstyring

Systemer til styring af adgangskoder
Så vidt muligt skal der benyttes IT-systemer, der automatisk kan styre de krav, der findes til adgangskoder i afsnit 9.3.1 Retningslinjer for adfgangskoder.
Adgangskontrolsystemet skal låse brugerkonti efter fire forgæves adgangsforsøg.

Retningslinier for adgangsstyring
Digitalisering & IT har det overordnede ansvar for at etablere og vedligeholde procedurer for adgangsstyring.

Registrering af brugere
- Brugere skal have unikt brugernavn og bruger-id.
- Digitalisering & IT skal tildele brugeradgang.

- Ledelsen skal godkende oprettelse og ændring af brugeradgang.
- Brugere skal modtage en skriftlig bekræftelse af de tildelte rettigheder.
- Digitalisering & IT skal vedligeholde fortegnelser over, hvordan bruger-ID eller rettigheder fjernes eller ændres ved ophør eller ændring af brugeres jobfunktion.
- Procedurer for autorisation af brugeradgang skal omfatte en formel autorisationsformular i hvilken de nødvendige privilegier specificeres.
- Autorisationer til brugerne skal godkendes elektronisk af lederen eller bemyndigede personer. Sendes til og opbevares af Digitalisering & IT som dokumentation.

Brugerprofiler for konsulenter og deltidsansatte
Personer, som er ansat eller har konsulentaftale, må oprettes som brugere.
Vikarer, praktikanter og timelønnede må oprettes som brugere. Ophører ansættelses- eller vikaraftale, skal brugerprofilen øjeblikkeligt nedlægges.

Medarbejderes omplacering
Ved omplacering af medarbejdere skal alle rettigheder for pågældende bruger revurderes.

Fratrædelse
Det er ledelsens ansvar, at ved fratrædelse bliver alle brugerprofiler og systemrettigheder nedlagt inden 14 dage.

9.1.1 Politik for adgangsstyring

Begrænset adgang til data
Brugere og medarbejdere med supportfunktioner må kun få adgang til systemfunktioner og data, hvis dette er forretningsmæssigt begrundet.

Adgangsbegrænsning til data
Applikationer skal sikre, at adgang til data sker efter beskrevne adgangsregler indeholdt i IT-sikkerhedspolitikken.

9.1.2 Adgang til netværk og netværkstjenester

Styring af netværksadgang
Digitalisering & IT skal ved styring af brugernes netværksadgang sikre imod uautoriseret anvendelse af fælles netværk og hertil knyttede tjenester.

Godkendelse ved adgang til netværket
Brugerens adgang til det interne netværk fra andre lokationer end kommunens skal benytte brugernavn, kodeord og SMS-passcode.
To-faktor godkendelse skal benyttes ved fjernadgang til det interne netværk.

Retningslinier for brug af netværkstjenester
Brugere skal kun have adgang til de tjenester, de er autoriseret til at benytte. Der henvises til forvaltningslovens § 32, der beskriver, ansattes mulighed for at anskaffe sig fortrolige oplysninger, som ikke er af betydning for den pågældendes opgaver.

Forbindelse til fremmede trådløse netværk

Hvis man skal bruge andre end kommunes netværk (private/offentlige netværk) skal man bruge internettet til at koble sig på Citrix. Har maskinen været brugt på andre end kommunens netværk skal denne sikkerhedstjekkes i Digitalisering & IT inden tilkobling på kommunes netværk, jf. afsnit 6.2.2.

Accepteret brug af data og systemer
Systemejere skal lave retningslinier for accepteret brug af kommunes data og systemer.

Adgang til trådløse netværk
Brugere skal godkendes ved hjælp af et brugernavn og password, før der gives adgang til kommunens trådløse netværk.

Overvågning af netværk
Digitalisering & IT skal have den nødvendige viden og redskaber til overvågning af kommunes netværk, for eksempel til fejlretning samt detektering og sporing af sikkerhedshændelser.
Digitalisering & IT skal løbende overvåge netværk med henblik på detektering af brud på IT-sikkerheden.
Digitalisering & IT skal årligt udføre evalueringer af regler for netværkstrafik i firewalls og routere.

Kapacitetsovervågning
Alle serversystemer skal overvåges døgnet rundt for tilstrækkelig kapacitet til at sikre pålidelig drift og tilgængelighed. Større afvigelser fra normal-kapacitet skal registreres og håndteres som en ikke normal hændelse.

Overvågning af internetforbindelser
Digitalisering & IT skal løbende overvåge internetforbindelser med henblik på at detektere elektroniske angreb.

9.1.3 Distancearbejdspladser

Distancearbejdspladser
En distancearbejdsplads er en netværksgodkendt arbejdsplads, der af kommunen er stillet til rådighed for en bruger på dennes private bopæl med henblik på, at brugeren fra distancearbejdspladsen helt eller delvist skal kunne udføre sine normale arbejdsmæssige funktioner. Politikerarbejdspladser er også at betragte som distancearbejdspladser. Distancearbejdspladsen udgør sit eget lille netværk, som er koblet op mod kommunens fælles netværk. For distancearbejdspladsen gælder samme forskrifter som for øvrige arbejdspladser tilsluttet netværket.

- Anvendelsen må som udgangspunkt kun ske ved benyttelse af de, af kommunen, installerede programmer og uden systemmæssige ændringer i øvrigt. Der vil dog i rimeligt omfang kunne installeres lovligt erhvervede private programmer, der umiddelbart vil kunne afvikles uden systemmæssige modifikationer, og som ikke medfører systemmæssige problemer eller urimelige krav til support fra Digitalisering & IT.
- Anvendelsen af arbejdspladsen må kun ske af brugeren selv, mens der er etableret forbindelse til det fælles netværk.
- Anvendelsen må ikke vedrøre brugerens private erhvervsvirksomhed eller anden erhvervsvirksomhed.
- Anvendelsen må ikke medføre gener for øvrige brugere på netværket, f.eks. i form af langvarige liniebelastninger.
- Anvendelsen må ikke udgøre nogen sikkerhedsrisiko i forhold til netværket.
- Anvendelsen må ikke medføre overtrædelse af gældende lovgivning eller være i modstrid med, hvad der anses for normal god skik og brug.

Undtagelser kan være gældende i et vist omfang, disse er udtrykkeligt beskrevet i nærværende IT-sikkerhedspolitik.

Det er ikke hensigten at begrænse den private anvendelse mest muligt, men at gøre den så sikker og uproblematisk som mulig.

9.2 Administration af brugeradgang

Retningslinier for adgangskoder
Ved brugeroprettelse eller nulstilling af adgangskode skal brugere tildeles en sikker, midlertidig adgangskode, som skal ændres umiddelbart efter første anvendelse.
Midlertidige adgangskoder skal være unikke, må ikke genbruges og skal opfylde de almindelige krav til adgangskoder.

9.2.1 Brugerregistrering og -afmelding

Det er Digitalisering & IT som opretter nye brugere. Det er den ansvarlige for godkendelsen af oprettelsen, som skal sende et brugerautorisationsskema til Digitalisering & IT, hvorefter den nye bruger registreres med de ønskede adgange.
Når en bruger skal afmeldes, udfyldes samme brugerautorisationsskema med slutdato, hvorefter det sendes til Digitalisering & IT, som sletter brugeren i systemet.

9.2.2 Tildeling af brugeradgang

Gennemgang af brugerprofiler
Digitalisering & IT gennemgår alle brugerprofiler mindst hver 6. måned for at identificere inaktive profiler eller tilsvarende, der skal fjernes eller ændres.

9.2.3 Styring af priviligerede adgangsrettigheder

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

Skift af administrator adgangskode ved fratrædelse
Hvis en person med kendskab til administrative adgangskoder fratræder, skal disse adgangskoder ændres med det samme.

Administratorbeskyttelse
Der skal benyttes systemadministrator-adgangskode på alle platforme.

Ændring af administrative adgangskoder
Administrative adgangskoder skal følge samme minimumsregler som øvrige adgangskoder.
Administrative adgangskoder skal ændres, hvis udenforstående får kendskab til disse.

9.2.4 Styring af godkendelsesdata om brugere

Identifikation af brugerprofiler for eksterne brugere
Bruger-id skal udarbejdes efter en standard navnekonvention. Dette gælder også for gæster, konsulenter og lignende, således at disse kan identificeres enkelt og ligetil.
Standardadgangskoder og bruger-id'er må ikke anvendes på kommunes systemer. Disse skal ændres eller

slettes.

Overdragelse af adgangskoder
Adgangskoder må ikke overdrages på ukrypterede forbindelser, for eksempel e-mail.
Midlertidige adgangskoder kan overdrages verbalt, for eksempel over telefonen.

9.2.5 Gennemgang af brugeradgangsrettigheder

Digitalisering & IT udtager hvert kvartal brugere og gennemgår de tildelte autorisationer og rettigheder, hvorefter de sendes til lederen, som godkender om medarbejderen har de korrekte adgange.

9.2.6 Inddragelse eller justering af adgangsrettigheder

Inddragelse af rettigheder ved fratrædelse
Der skal forefindes en procedure for inddragelse af rettigheder i forbindelse med fratræden eller afskedigelse af personale.
Proceduren for inddragelse af rettigheder skal indeholde en liste over funktioner og personer, der skal informeres i forbindelse med fratrædelsen.

9.3 Brugernes ansvar

9.3.1 Retningslinjer for adgangskoder

Brug af autologin funktioner
På eksterne websites må browserens indbyggede funktion anvendes, såfremt denne funktion er beskyttet af adgangskoder.

Valg af sikre kodeord
En bruger må ikke kunne vælge en adgangskode, der er identisk med en af de seks senest benyttede adgangskoder.

Genbrug af adgangskoder
Adgangskoder må genbruges på interne og eksterne systemer.

Adgangskoder er strengt personlige
Adgangskoder er strengt personlige og må ikke deles med andre.

Skift af adgangskoder
Adgangskoder skal skiftes mindst en gang årligt.

Indhold af adgangskoder
Adgangskoder skal indeholde kombinationer fra mindst to af følgende kategorier: Store bogstaver, små bogstaver, tal og specialtegn.
Der må ikke benyttes brugernavn, navn eller datoer som en del af adgangskoder.

Længde af adgangskoder
Adgangskoder skal være mindst 8 tegn langt.

9.4 Styring af system- og applikationsadgang

9.4.1 Begrænset adgang til data

Adgang til funktionalitet og data i IT-systemer
IT-systemer skal overholde kommunes regler for adgangskontrol indeholdt i IT-sikkerhedspolitikken.
Reglerne for adgangskontrol på de enkelte systemer skal baseres på en risikovurdering og på de forretningsmæssige behov

9.4.2 Procedurer for sikker login

Sikre login-procedurer skal indbefatte:
- At data fra systemet eller applikationen ikke vises ved login.
- At brugeren skal udfylde alle felter, før login accepteres.
- Beskyttelse mod brute-force login-forsøg.
- Logning af succesfulde login-forsøg.
- Logning af mislykkede login-forsøg.
- Oprettelse af en sikkerhedshændelse, hvis der registreres en overtrædelse af login-procedurerne.
- Ved succesfuld login, visning af tid og dato for seneste login.
- Ved succesfuld login, visning af antal mislykkede forsøg siden sidste login.
- At indtastede adgangskoder ikke vises.
- At der ikke sendes adgangskoder i klartekst over netværk.

9.4.3 System for administration af adgangskoder

System til håndtering af adgangskoder
Lemvig Kommune har ikke implementeret et adgangskodesystem (single sign on).

Implementering af et system til håndtering af adgangskoder
Der skal implementeres et adgangskodehåndteringssystem for kritiske systemer, der håndhæver virksomhedens adgangskoderegler.

9.4.4 Brug af priviligerede systemprogrammer

Brug af systemværktøjer
Digitalisering & IT skal begrænse og styre adgangen til systemværktøjer, der kan påvirke eller omgå systemers eller enheders sikkerhed.
Digitalisering & IT skal sikre, at unødige systemværktøjer ikke er installeret eller tilgængelige på brugeres pc'er.
Digitalisering & IT skal sikre, at brugen af systemværktøjer begrænses til et minimum af betroede og autoriserede brugere.

9.5 Mobilt udstyr og fjernarbejdspladser

9.5.1 Politik for mobilt udstyr

Adgang til bærbare computere
Adgang til bærbare computere skal beskyttes med kodeord.

Opsyn med mobile enheder
Adgang til mobile enheder skal beskyttes med et kodeord.
Mobile enheder må ikke efterlades uden opsyn i uaflåste rum.

Kameraer
Kameraer, for eksempel i mobiltelefoner og andet udstyr, må kun i arbejdsrelateret øjemed anvendes i kommunens sikre zoner (serverrum).

Ejere af data på mobile enheder
På mobile enheder med en primær ejer er pågældende ansvarlig for data.

Ansvar for sikkerheden på IT-platforme
Digitalisering & IT er ansvarlig for IT-sikkerheden på de anvendte platforme. Kontroller skal implementeres og defineres i samråd med systemejerne.

9.5.2 Fjernarbejdspladser

Fjernarbejdspladser defineres som distancearbejdspladser og arbejde foretaget på mobile enheder jf. 9.1.3.

Adgang fra distancearbejdspladser
Adgang gives kun for godkendte brugere med brugernavn, kodeord samt SMS-passcode.

Forsikringsdækning for mobile enheder
Økonomi & HR skal sikre, at der er etableret passende forsikringsdækning i forbindelse med opbevaring og anvendelse af IT-udstyr uden for kommunens lokaliteter.

Usikker enhed Rød
En enhed som betegnes usikker(Rød), er en enhed, der ikke har eller må have direkte adgang til kommunes netværk.
For at tilkoble sig kommunes netværk på en usikker(Rød) enhed, skal der benyttes Citrix samt SMS-passcode.
På en usikker (Rød) enhed stillet til rådighed af kommunen gælder samme retningslinjer som på en sikker (Grøn) enhed.
Det vil sige, at anvendelsen, som udgangspunkt, kun må ske ved benyttelse af de af kommunen installerede programmer og uden systemmæssige ændringer i øvrigt. Der vil dog i rimeligt omfang kunne installeres lovligt erhvervede private programmer, der umiddelbart vil kunne afvikles uden systemmæssige ændringer.
Installation skal altid ske med forud indgået aftale med Digitalisering & IT.
Distancearbejdsplads og en politikerarbejdsplads betegnes også som værende en usikker (Rød) enhed udleveret af
kommunen, da disse ikke har direkte adgang til kommunes netværk.

En usikker (Rød) enhed kan være:
- En bærbar PC som bruges på flere netværk.
- En IPad.
- En Smartphone.

Sikker enhed Grøn (Domæne tilmeldt)
En sikker enhed har direkte adgang til kommunes netværk. Denne enhed betegnes som en netværksgodkendt enhed, som kommunen har stillet til rådighed. En sikker (Grøn) enhed må kun benyttes på kommunes netværk og må
ikke tilkobles andre netværk herunder hjemmenetværk, offentlige trådløse netværk.
På en sikker (Grøn) enhed må der ikke installeres programmer eller foretages ændringer uden Digitalisering &

IT´s
medvirken.

En sikker (Grøn) enhed kan være:

- En terminal
- En PC
- En bærbar PC, som kun bruges på kommunens netværk trådløst, via kabel eller bruger mobilbredbånd til direkte opkobling mod kommunes netværk uden SMS-passcode.

Enhederne mærkes således at det tydeligt fremgår om enheden er Grøn (sikker) eller Rød (Usikker). Digitalisering og IT foretager mærkningen ved udlevering af enheden.

10 Kryptografi

Kommunen skal efterleve de nationale regler for kryptografering. Dette gælder også for medarbejdere der besøger andre lande, medbringende bærbart og mobilt udstyr.

10.1 Kryptografiske kontroller

10.1.1 Politik for anvendelse af kryptografi

Brug af kryptering i forbindelse med opbevaring af data
Fortrolige informationer skal altid være krypteret, når de opbevares på transportabelt udstyr, fx på bærbare computere samt håndholdte enheder som tablets og mobiler.

10.1.2 Administration af krypteringsnøgler

Nøglehåndtering
Digitalisering & IT skal etablere et nøglehåndteringssystem, som understøtter virksomhedens anvendelse af kryptografi.

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

11 Fysisk sikring og miljøsikring

Fysisk sikkerhed og adgangsregler er naturlige elementer i kommunens IT-sikkerhedspolitik. Fysisk sikkerhed omfatter blandt andet døre, vinduer, alarmer- samt tyverisikring af kommunens fysiske aktiver, eksempelvis IT-udstyr. Systemer til adgangskontrol er ligeledes et element af fysisk sikkerhed, der sikrer, at kun personer med legalt ærinde får adgang til kommunens område.

11.1 Sikre områder

Sikre områder er områder, hvor der opbevares og behandles fortrolige oplysninger, bl.a. kontorer, serverrum og lignende.

11.1.1 Fysisk sikring

Indbrudsalarmer

Der skal anvendes tilstrækkelige alarmsystemer i alle lokaler med IT-udstyr, der indeholder fortrolige informationer.

Adgang til serverrum og IT-klargøringsrum
Chefen for Digitalisering & IT er ansvarlig for godkendelse af personale med adgang til serverrum og IT-klargøringsrum.

Oplysninger om sikre områder
Oplysninger om sikre områder og deres funktion skal alene gives ud fra et arbejdsbetinget behov.

Sikring af kontorer, lokaler og udstyr.
Ledelsen må uddelegere ansvaret for at sikre en passende fysisk sikring af kontorer, rum og udstyr bliver implementeret og vedligeholdt.

Ansvar for den fysiske adgangskontrol
Ledelsen er ansvarlig for at kontrollere fysisk adgang til kommunens faciliteter. Dette ansvar kan delegeres til betroede medarbejdere.

11.1.2 Beskyttelse mod eksterne og miljømæssige trusler

Sikring
Serverrum, krydsfelter og tilsvarende områder skal sikres mod eksterne trusler og miljømæssige hændelser som vand, brand, eksplosion og tilsvarende påvirkninger.
Serverrum skal sikres med veldimensioneret brandslukningsudstyr og serverrum må ikke benyttes som lager for brændbare materialer.
Farlige eller brandfarlige materialer skal lagres i sikker afstand fra sikre områder.

11.1.3 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. Sidste medarbejder der forlader et område er ansvarlig for sikring af dette.

11.1.4 Områder til af- og pålæsning

Af- og pålæsningsområder skal indrettes så risiko for uautoriseret adgang til kommunens øvrige områder mindskes.

11.2 Udstyr

11.2.1 Placering og beskyttelse af udstyr

Adgang til serverrum og hovedkrydsfelter
Adgang til serverrum og hovedkrydsfelter tillades kun med sikkerhedsgodkendelse eller ved overvåget adgang af medarbejdere fra Digitalisering & IT.

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

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

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

11.2.2 Understøttende forsyninger (forsyningssikkerhed)

Køling
Serverrum skal sikres med veldimensionerede airconditionanlæg.

Nødstrømsanlæg
Alle forretningskritiske systemer skal beskyttes med nødstrømsanlæg med kapacitet til mindst 15 minutters uafbrudt drift.

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

Opbevaring af bærbare enheder
Bærbare enheder skal fjernes eller låses inde efter arbejdstids ophør.

Misbrugsbeskyttelse af IT-udstyr
Ledelsen skal sikre, at medarbejdere informeres om eventuelle overvågningsmuligheder, som kommunen kan tage i brug.
Anvendelse af IT-udstyr til uautoriserede formål uden tilladelse må ikke finde sted.

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
Systemejere/Digitalisering & IT skal vedligeholde udstyr efter leverandørens anvisninger. Kun godkendte leverandører må udføre reparationer og vedligeholdelse.
Digitalisering & IT er ansvarlig for, at der føres log over alle fejl og mangler samt reparationer og forebyggende vedligeholdelse.

11.2.5 Fjernelse af aktiver

Fjernelse af udstyr fra kommunen
Udstyr må kun fjernes fra kommunen, hvis der foreligger en aftale om udlånet og udlånsperioden skal være aftalt.
Udstyr der indeholder fortrolige data, må kun fjernes efter behørig godkendelse fra pågældende dataejer.

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 og der skal udvises forsigtighed ved omtale af fortrolige informationer i offentlige rum.

11.2.7 Sikker bortskaffelse eller genbrug af udstyr

Bortskaffelse eller genbrug af udstyr
Når udstyr bortskaffes eller genbruges skal kritiske/følsomme informationer og licensbelagte systemer fjernes eller overskrives. Dette foretages af Digitalisering & IT.

Bortskaffelse og genbrug af medier
Alle datamedier, for eksempel harddiske, disketter, cd, dvd, bånd og hukommelsesenheder, skal sikkerhedsslettes eller destrueres inden bortskaffelse. Sletning og bortskaffelse foretages af Digitalisering & IT.

11.2.8 Brugerudstyr uden opsyn

Placering af udstyr
Udstyr skal placeres eller beskyttes, så risikoen for skader og uautoriseret adgang minimeres. Udstyr der benyttes til at behandle kritiske/følsomme informationer skal beskyttes og placeres, så informationerne ikke kan ses af uvedkommende.

11.2.9 Politik for ryddeligt skrivebord og blank skærm

Brug af kodeordsbeskyttet pauseskærm
Når brugeren forlader arbejdsstationen således, at den er uden for brugerens synsvidde, skal brugeren aktivere kodeordsbeskyttet skærmlås. Adgangskodebeskyttet skærmlås skal aktiveres på pc-arbejdspladser efter 15 minutters inaktivitet.

Opbevaring af fysiske dokumenter
Dokumenter indeholdende personoplysninger skal opbevares så det sikres, at uvedkommende ikke har adgang til disse.

12 Driftssikkerhed

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.

12.1 Driftsprocedurer og ansvarsområder

12.1.1 Dokumenterede driftsprocedurer

Krav til driftsafviklingsprocedurer
Driftsafviklingsprocedurer for systemer, der er forretningskritiske, skal være dokumenterede, ajourførte og tilgængelige for driftsafviklingspersonalet og andre med et arbejdsbetinget behov.

Driftsansvar
Digitalisering & IT står for den daglige drift, administration og sikkerhed af fælles IT-systemer. Herunder efterlevelsen af sikkerhedspolitikker, regler og procedurer der er relevant for IT-driften.

Dokumentation
Digitalisering & IT skal sikre, at alle systemer og IT-relaterede forretningsgange er dokumenterede for eksempel ved, at systemejere og procesejere dokumenterer i henhold til kommunens standard.

Deaktivering af beskyttelsesmekanismer
Det er under ingen omstændigheder tilladt at deaktivere eller omgå kommunens beskyttelsesmekanismer, herunder anti-virus produkter. I særlige tilfælde kan Digitalisering & IT deaktivere disse.

Sikring af serversystemer
Alle servere skal sikres inden ibrugtagning.

Sikring af arbejdsstationer inden ibrugtagning
- Alle arbejdsstationer skal sikres inden brug. Minimumssikring inkluderer installation af seneste sikkerhedsrettelser for operativsystemet og anti-virus program.
- Alle arbejdsstationer skal installeres ved brug af den, af Digitalisering & IT, fastlagte procedure.
- Alle personlige computere, arbejdsstationer og lignende skal sikres af Digitalisering & IT inden brug.

Brugerne må ikke omgå denne sikring.

Registrering af driftsstatus
Digitalisering & IT skal registrere væsentlige forstyrrelser og uregelmæssigheder i driften af systemerne samt årsager hertil.

Sikkerhed i systemplanlægning
IT-sikkerhedskrav skal tages i betragtning ved design, testning, implementering og opgradering af nye IT-systemer samt ved systemændringer.

Integration af informationssystemer
Hvis integration af informationssystemer resulterer i en forøget risiko, skal den følge den normale procedure for godkendelse af IT-systemer.

12.1.2 Ændringsstyring

Ændringsstyring af IT-systemer
- Ved ændringer, f.eks. ved opdatering af systemer, 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 ændringen før arbejdet med den går i gang.
- Autoriserede brugere skal acceptere ændringer før de implementeres.
- Systemdokumentation skal opdateres ved hver ændring.
- Forældet systemdokumentation skal arkiveres eller destrueres.
- Driftsdokumentation og forretningsgange for brugerne skal holdes opdateret, således at de stadig er gældende efter ændringen.
- Implementeringen af ændringen skal foretages på et aftalt tidspunkt, så den forstyrrer de involverede parter mindst muligt.

Planlægning, test og godkendelse af ændringer
Ændringernes konsekvenser skal vurderes inden drift.

Retningslinier for ændringer
- Digitalisering & IT har ansvaret for, at der foregår en entydig identifikation og registrering af væsentlige ændringer.
- Information omkring udførte ændringer skal formidles til interessenter.
- Digitalsering & IT har ansvaret for, at der findes en nødprocedure til at mindske effekt fra fejlslagne ændringer.

12.1.3 Kapacitetsstyring

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

12.1.4 Adskillelse af test/udvikling og driftsmiljøer

Sikring af applikationsudviklingsmiljøerne
Test/udviklingsmiljøer skal sikres mod trusler som uautoriseret adgang, ændringer og tab. Data skal sikres efter følsomhedsniveau.

12.2 Beskyttelse mod malware

12.2.1 Kontroller mod malware

Kontrol af antivirus på arbejdsstationer
Hvis medarbejdere bliver opmæksom på, at anti-virus ikke er aktivt, skal de kontakte Digitalisering & IT, som bringer dette i orden.

Antivirus produkter på arbejdsstationer
Digitalisering & IT skal sikre, at der anvendes minimum to anti-virus produkter fra forskellige leverandører. Ét på indgangene til kommunens systemer og et andet på samtlige computere ejet af kommunen. Opdatering skal ske højest et døgn efter leverandørens opdateringer eller ved næste tilkobling til netværket.

Spyware
Digitalisering & IT skal sikre, at der regelmæssigt scannes for spyware på alle arbejdsstationer.

Adware
Adware-beskyttelse baseres på medarbejderopmærksomhed og sikkerhedsindstillinger i internetbrowser, begrænsninger i brugeres muligheder for softwareinstallation samt brug af adware-scannere. Digitalisering & IT skal sikre, at der regelmæssigt scannes for adware på alle arbejdsstationer.

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

Antivirusprogrammer

Anti-virusprogrammer skal være installeret på sikre og usikre enheder. Softwaren skal jævnligt holdes opdateret.

12.3 Backup

12.3.1 Backup af information

Sikkerhedskopiering af data på serversystemer
Digitalisering & IT er ansvarlig for sikker lagring og backup af data på serverudstyr.

Afprøvning af procedurer for sikkerhedskopiering
Muligheden for at reetablere data fra backup-systemer skal regelmæssigt aftestes.

Sikkerhedskopiering af data på andre systemer
Såfremt forretningskritiske data ikke opbevares på serversystemer, skal dataejer være ansvarlig for etablering af relevant sikkerhedskopiering.

Opbevaring af sikkerhedskopier på ekstern lokation
Datamedier til reetablering af forretningskritiske systemer skal opbevares på et, i forhold til systemernes placering, eksternt opbevaringssted.
Reserveanlæg, udstyr og datamedier med sikkerhedskopier skal opbevares i sikker afstand for at undgå skadevirkninger fra et uheld på det primære anlæg.

12.4 Logning og overvågning

12.4.1 Hændelseslogning

Opfølgningslogning
- Digitalisering & IT skal logge sikkerhedshændelser på kommunens systemer, hvor der er individuel brugerlogin.
- Digitalisering & IT skal logge fejlhændelser på kommunens væsentlige systemer.
- Digitalisering & IT skal endvidere logge væsentlige brugeraktiviteter på kommunens væsentlige systemer.

Opfølgningsloggen skal indeholde følgende
- Brugerindentifikation.
- Dato og klokkeslæt for væsentlige aktiviteter.
- Identificering af arbejdsstation og netværksenhed.
- Registrering af systemadgange og forsøg herpå.
- Alarmer fra agangskontrolsystem.

Opbevaring af opfølgningslog
Digitalisering & IT skal opbevare log for sikkerhedshændelser på kommunens systemer, hvor der er individuel brugerlogin i mindst 6 måneder.
Direktionssekretariatet skal opbevare log for brugerhændelser på kommunens systemer, hvor der er individuel brugerlogin i mindst 6 måneder.
Opfølgningsloggen skal journaliseres.

Fejllog

Fejl skal logges og om nødvendigt analyseres. Nødvendige udbedringer og modforholdsregler skal gennemføres.

Overvågning af internetbrug
Den enkelte medarbejders anvendelse af internet bliver logget. Kommunen har mulighed for at filtrere og begrænse internetadgang.

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

12.4.2 Beskyttelse af logoplysninger

Beskyttelse af logoplysninger
Logfaciliteter og logoplysninger skal beskyttes mod manipulation og tekniske fejl.

12.4.3 Administrator- og operatørlog

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

12.4.4 Tidssynkronisering

Tidssynkronisering
Digitalisering & IT skal sikre at systemernes ure jævnligt synkroniseres til korrekt tid.

12.5 Styring af driftssoftware

12.5.1 Softwareinstallation på driftsystemer

Krav til indstillinger af internet-browser
Microsoft Internet Explorer skal altid være konfigureret iht. Digitalisering & ITs standard eller med højere sikkerhedsindstillinger.

Installation af programmer på arbejdsstationer
Operativsystemer og applikationer må kun installeres og ændres af Digitalisering & IT på godkendt udstyr. Anvendelsen af ikke godkendt udstyr mv. kan resultere i disciplinære sanktioner.

Softwareopdateringer generelt
Digitalisering & IT skal holde sig informeret om alle programrettelser til alle programmer, der anvendes på kommunens udstyr. Disse skal installeres på alle kommunens computere. For eksempel på servere og arbejdsstationer, når det vurderes, at rettelserne har positiv indflydelse på den samlede sikkerhed.

Ændringer i systemer, der er forretningskritiske.
Alle ændringer i systemer, der er forretningskritiske, skal 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.

Forbudte og tilladte programmer

Ingen brugere må på netværket anvende ikke tilladte programmer. Ingen brugere må på netværket lagre eller opbevare programmer, hvis det ikke, i den enkelte situation, sker på udtrykkelig foranledning af Digitalisering & IT.

12.6 Sårbarhedsstyring

12.6.1 Styring af tekniske sårbarheder

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

Rettelser til operativsystemer
Digitalisering & IT skal løbende vurdere tilgængelige sikkerhedsrettelser, for eksempel "patches" eller "hot-fixes", til anvendte operativsystemer. Udrulning/installation skal foretages efter behov.

Rettelser til applikations-programpakker
Digitalisering & IT skal mindst hver uge vurdere tilgængelige sikkerhedsrettelser ("patches" eller "hot-fixes"). Udrulning/installation skal foretages efter behov.

Større operativsystemopdateringer
Når større opdateringer, for eksempel "service packs", er gjort tilgængelige fra leverandører, skal Digitalisering & IT-afdelingen vurdere, om disse skal installeres.
Større opdateringer skal testes grundigt for kompatibilitet med anvendte applikationer, inden opdateringerne installeres i produktionsmiljøet.

Større programpakkeopdateringer, for eksempel "service packs"
Større opdateringer skal testes i et testmiljø, inden opdateringerne installeres i produktionsmiljøet.

12.6.2 Begrænsninger på softwareinstallation

Sikkerhedsindstillinger i web-browser
Websites på internet må kun besøges med sikkerhedsindstillinger mindst sat til "medium" for internetzonen. Der må kun anvendes godkendte webbrowsere. Brugerne må ikke forsøge at omgå eller bryde sikringsforanstaltningerne.

Administration af administratorrettigheder
Administratoradgangskoder må ikke gives til andre end medarbejdere i Digitalisering & IT. Dispensation gives kun af Chefen for Digitalisering & IT.

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 kommunens aktiviteter.
De personer, der udfører revisionen, skal være uafhængige af det reviderede område.

Beskyttelse af revisionsværktøjer

Adgangen til revisionsværktøjer skal begrænses for at forhindre misbrug.

13 Kommunikationssikkerhed

Kommunikationssikkerheden er et vigtigt element i IT- sikkerhedspolitikken, da der arbejdes med personfølsomme data.

13.1 Styring af netværkssikkerhed

13.1.1 Netværksstyring

Installation af trådløst udstyr
Medarbejdere må ikke installere eller ibrugtage udstyr, der giver trådløs netadgang.

Indkommende netværksforbindelser
Der tillades kun etablering af forbindelser fra internet til sikkerhedsgodkendte servere, eksempelvis til e-mail og webservere.

Udgående netværksforbindelser
Digitalisering & IT er ansvarlig for, at der er etableret de nødvendige restriktioner på forbindelser fra det interne netværk til internet eller andre netværk.

Ansvar for internetforbindelser
Det overordnede ansvar for internetforbindelserne ligger hos Digitalisering & IT.

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

Sikring af netværk
Digitalisering & IT har det overordnede ansvar for at beskytte kommunens netværk.

Adgang til aktive netværksstik
Adgang til aktive netværksstik skal styres af Digitalisering & IT.

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

Tilslutning af udstyr til netværk
Det er tilladt, at ansatte kobler godkendt sikkert udstyr til netværket, efter aftale med Digitalisering & IT. Udstyret må ikke forstyrre driften, og Digitalisering & IT kan kræve det frakoblet.

Rutekontrol
Digitalisering & IT skal:

- Begrænse rutning imellem forskellige netværkssegmenter, således at kun nødvendig trafik videresendes.
- Overveje anvendelsen af filtrering på afsender- og modtager-adresser på relevante protokoller imellem alle relevante netværkssegmenter
- Sikre passende netværks- eller node-autentificering til ethvert netværkssegment.

Personlige firewalls
Alle arbejdsstationer skal benytte firewalls.

Firewall-funktioner på servere
Alle servere med indbygget firewall funktionalitet skal benytte denne til at sikre, at der kun gives adgang til nødvendige services.

Opdeling af netværk
Digitalisering & IT skal segmentere netværk for at etablere en passende adskillelse imellem forskellige tjenester, brugergrupper eller systemer.
Mindste krav til netværkssegmentering er, at Digitalisering & IT 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.

Kryptering af administrative netværksforbindelser
Forbindelser, der benyttes til IT-administration, skal krypteres, hvis de benytter offentlige eller usikre netværk for eksempel internettet.

Placering af trådløse netværk
Trådløst udstyr må kun forbindes til den eksisterende infrastruktur ved hjælp af sikkerhedsgodkendt firewall.

Adgang til trådløse netværk for gæster
Gæster må få udleveret brugernavn og password til gæstenettet.
Gæster må tilslutte eget udstyr trådløst til gæstenettet, forudsat at udstyret ikke generer andre systemer.

Brug af trådløse lokalnetværk
Kun brug af trådløse netværk, som er opsat af eller på foranledning af Digitaliering & IT tillades.
Brug af trådløse netværk tillades, når "access point" befinder sig på et lokalnetværkssegment, der er sikkert (f.eks. ved hjælp af en firewall) adskilt fra sikre lokalnetværkssegmenter.

Adgang til netværket via mobilt udstyr
Adgangen til kommunens netværk må kun ske gennem sikkerhedsgodkendte løsninger.

Adgang til applikationer på kommunens netværk
Der er også adgang til kommunes programmer ved fjernadgang.

Sikkerhedskontroller overfor fjernopkoblet udstyr.
Relevante mobile enheder skal sikres med antivirus, firewall og adgangskontrolsystemer. Disse foranstaltninger skal opdateres løbende.

Distancearbejdspladser
Tillades når sikkerhedspolitikken i øvrigt overholdes.

Opbevaring af fortrolige informationer
Der må ikke behandles eller opbevares personhenførbare eller fortrolige informationer på andet udstyr end kommunens computere.

Personligt ejet IT-udstyr som pc, tablets, bærbare harddiske, memorysticks, MP3-afspillere, minidisks, cd- eller dvd-brændere må ikke anvendes til kopiering eller opbevaring af fortrolige data.

13.1.2 Sikring af netværkstjenester

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

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

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.

Afvikling af programmer i forbindelse med internetsurfing
Det er tilladt at afvikle browserbaserede programmer, forudsat at disse er digitalt signerede, således at programleverandøren tydeligt fremgår.

Internetbaserede tjenester
Digitalisering & IT vedligeholder en liste over de internetbaserede tjenester, der ikke er godkendte.

Adgang til surfing på internettet
Netværket må gerne bruges til internet-browsing.

Medarbejderes private brug af internetadgang
Kommunens internetadgang bruges som udgangspunkt kun arbejdsrelateret, såfremt sikkerhedspolitikken i øvrigt overholdes, og såfremt arbejdsrelateret brug ikke generes på nogen måde.

Streaming via internet
Det er ikke tilladt at anvende kommunens netværk til tung og vedvarende trafik, som eksempelvis radio- og tv-tjenester samt film med mindre det er fagligt relevant.

Download af filer fra internet
Der må kun efter forudgående aftale med Digitalisering & IT hentes filer fra internettet. Filerne må kun hentes og benyttes arbejdsmæssigt og de skal specifikt scannes for virus umiddelbart efter download og inden de åbnes.

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

Mulighed for "kigge med" funktion

Det er tilladt at benytte krypterede sessioner, for eksempel Secure Shell (SSH), fra det interne netværk til andre netværk.

Fjernstyring og -administration
Det er tilladt at benytte værktøjer til fjernadministration, hvis der foreligger sikkerhedsgodkendelse af produktet og opkoblingsformen.

13.2 Informationsoverførsel

13.2.1 Politikker og procedurer for informationsoverførsel

Udlevering af fortrolige informationer og oplysninger
Fortrolig information må ikke videregives til tredjepart i nogen form, hvis videregivelse ikke lever op til lovgivningens krav, bl.a. Persondataforordningens §6. Hvis der skal ske videregivelse skal systemejeren godkende dette.

Elektroniske dokumenter
Elektroniske kopier af dokumenter, for eksempel indscannede dokumenter og faxer, med fortrolige eller følsomme informationer, må kun behandles og lagres på kommunens IT-udstyr.

Procedurer for informationsudveksling
Chefen for Digitalisering & IT har ansvaret for, at der foreligger retningslinier og procedurer for enhver form for elektronisk informationsudveksling.

Udskrivning
Printere, som benyttes til udskrivning af fortrolige informationer, skal placeres, så de ikke er generelt tilgængelige. Der skal anvendes udskrivningskode på alle kommunens printere.

13.2.3 Elektroniske meddelelser

Sagsbehandling og journalisering af e-mail
Modtaget og afsendt e-mail skal journaliseres og behandles efter samme principper, som gælder for almindelig brevpost og fax.

Brug af chat- og beskedprogrammer
Det er tilladt at bruge godkendte programmer, hvis det benyttes arbejdsrelateret. Chat-meddelelser er omfattet af regler om journalisering og behandles efter samme principper, som gælder almindelig post.

Overholdelse af markedsføringsloven
Direktionen skal sikre, at organisationen efterlever markedsføringsloven på alle områder.

Identifikation af relevant lovgivning
Direktionen er ansvarlig for at identificere lovgivning, der er relevant for kommunens drift, eller udpege en person, der er ansvarlig for denne opgave.
Direktionen er ansvarlig for, at alle eksterne sikkerhedskrav og kommunens håndtering heraf, klarlægges, dokumenteres og løbende vedligeholdes.

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-programmer.

Ejerskab
Kommunen betragter alle e-mails som kommunens ejendom.

Vedhæftede filer
Programfiler og kommando-filer må ikke vedhæftes eller åbnes. Det gælder eksempelvis følgende filtyper: .exe, .com, .scr, .pif, .bat, cmd, .vbs.
Digitalisering & IT skal blokere for filtyper, som de vurderer for farlige eller uhensigtsmæssige.
Kun dokumentfiler, billedfiler og arkiver må vedhæftes og åbnes. Tilladte filtyper fremgår af listen over tilladte filtyper som vedligeholdes af Digitalisering & IT.

Fortrolig mail
E-mail med følsomt indhold skal krypteres med godkendt software. Dette gælder især for klassificeret, fortrolig eller intern information, der sendes over internet.
E-mails med fortrolige eller følsomme personoplysninger (oplysninger omfattet af persondataforordningens artikel 1-4) skal altid krypteres, når de sendes over internettet eller andre åbne netværk.

Elektronisk udveksling af post og dokumenter
Hvis e-mail bruges til bindende aftaler, skal de underskrives med en digital signatur.

Opbevaring og sletning af e-post
E-mail, der indeholder personhenførbare oplysninger, skal behandles i overensstemmelse med Persondataforordningen.

Phishing og bedrageri
Brugere skal være opmærksomme på "phishing" og "social engineering", der for eksempel kan betyde, at de modtager tilsyneladende oprigtige e-mails, der forsøger at franarre personlige eller fortrolige oplysninger, eller forsøger at få brugeren til at foretage uønskede handlinger.

Privat brug af e-mail
Kommunen tillader brug af e-mailsystemer til privat brug i rimeligt og begrænset omfang, såfremt IT-sikkerhedspolitikken i øvrigt overholdes. Kommunen forbeholder sig ret til at skaffe sig adgang til data og e-mail for brugerne, hvis dette sker af drifts- eller sikkerhedshensyn. Kommunen vil så vidt muligt forsøge at undgå at åbne eventuel privat e-mail-korrespondance.

Brug af previewfunktion til åbning af e-mail
E-mail må ikke vises i previewfunktion (Læserude må ikke være aktiveret).

14 Anskaffelse, udvikling og vedligeholdelse af systemer

Indkøb, udvikling og vedligeholdelse af systemer i kommunen skal foregå kontrolleret for at undgå en unødvendig forøgelse af risikoen for IT-sikkerheden. Når løsninger implementeres bør sikkerhedsovervejelser altid indgå som en integreret del af processen.

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 IT-sikkerhedspolitikken. Anskaffelser må ikke give anledning til forøget risiko for sikkerhedshændelser, med mindre Direktionen accepterer den øgede risiko.
Ethvert nyt system skal risikovurderes inden ibrugtagning.
Anskaffelse og installation af nyt IT-udstyr og -systemer skal godkendes af Chefen for Digitalisering & IT i henhold til fastlagt procedure.

14.1.2 Sikring af applikationer på offentlige netværk

Data integritet og fortrolighed skal sikres, når der benyttes applikations-services over offentlige netværk med kryptografiske løsninger såsom SSL, SFTP, HTTPS, sikre API'er eller webservices.

14.2 Sikkerhed i udviklings- og hjælpeprocesser

14.2.1 Sikker test/udviklingspolitik

Funktionsadskillelse i test/udvikling og driftsmiljøer

Der skal være funktionsadskillelse henholdsvis i forhold til test/udvikling og driftsmiljøet.
Funktionsadskillelse opnås ved brug af autorisationer.

Sikring af udviklingsmiljøer

Udviklingsmiljøer skal specielt sikre integritet i udviklingsprocessen, herunder sikring mod tab af data.
Ved risikovurdering af systemudvikling bør følgende overvejes:

- Omfanget af følsom data.
- Lovkrav.
- Adskillelse af udviklings-, test og produktionsmiljøer.
- Politikker for adgangskontrol og revisionsspor.
- Sikker udveksling af data mellem udvikling, test og produktion.
- Sikker lagring af backup.
- Revisionsspor af ændringer i miljøer.

Sikkerhedskravene bør identificere alle relevante sikkerhedsaspekter såsom beskyttelse af data der lagres, transporteres eller benyttes.
Analysen af sikkerhedskrav skal desuden tage hensyn til følgende:

- Krav til adgangstildeling og godkendelsesprocesser.
- Understøttelse af rollebaseret adgang.
- Krav fra andre systemgrænseflader.
- Krav til logning.
- Kompatibilitet med andre systemer og sikkerhedsløsninger.

14.2.2 Procedurer for styring af systemændringer

Styring af ændringer

Proceduren for ændringshåndtering skal omfatte test af den operationelle funktionalitet i forbindelse med den enkelte ændring.
Overgang fra udvikling til drift skal undergå test og kontrol for at tilsikre driftsniveau, sikkerhedsniveau og brugbarhed inden implementering. Derudover skal godkendt software sikres mod efterfølgende uønskede ændringer.

14.2.3 Teknisk gennemgang af programmer 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 den 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 og udføres kun af Digitalisering & IT eller i samarbejde med eksterne parter.

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 opgradering.

Anskaffelser
Digitalisering & IT skal tilse, at kun kendt og sikkert udstyr eller software med et defineret formål må anskaffes og tages i drift.
Indkøb, udvikling og implementering af nye systemer i kommunen skal foregå kontrolleret for at undgå en unødvendig forøgelse af risiko for IT-sikkerheden. Når løsninger implementeres bør sikkerhedsovervejelser altid indgå som en integreret del af processen.
Udstyr og software må kun indkøbes igennem Digitalisering & IT.

Kravspecifikation skal omhandle følgende områder
- Adgangskontrol.
- Alle væsentlige hændelser logges og overvåges.
- Beskyttelse mod fortrolighedskrænkelser i det omfang systemet skal behandle fortrolige eller personhenførbare informationer.
- Overholdelse af relevante love eller kontrakter.
- Mulighed for backup af data og system.
- Mulighed for genetablering efter kritiske, uforudsete fejlsituationer.
- Krav til viden og uddannelse af driftspersonale.

14.2.7 Outsourcet udvikling

Systemudvikling udført af ekstern leverandør
Kommunen kræver afleveringstest og dokumenteret løbende kvalitetssikring.

Ekstern revision af outsourcingpartnere
Relevante outsourcingpartnere skal sørge for ekstern revision mindst en gang om året.

Outsourcing
Ved outsourcing af IT-systemer skal Chefen for Digitalisering & IT inden indgåelse af kontrakt indhente information om sikkerhedsniveau fra outsourcingpartner og godkende, at kommunens sikkerhed samlet set ikke forringes af outsourcing.

Outsourcingpartnere
Inden indgåelse af aftaler skal sikkerhedsniveauet ved leverandøren afklares og sammenlignes med de krav, der stilles i sikkerhedspolitikken.

14.2.8 Systemsikkerhedstest

Godkendelse af nye eller ændrede systemer
Digitalisering & IT skal etablere en godkendelsesprocedure for nye systemer, versioner og for opdateringer af eksisterende systemer samt de afprøvninger, der skal foretages, inden de kan godkendes og sættes i drift. Godkendelsesproceduren skal sikre, at standardværdier, eksempelvis standard administrator-logins og andre "fabriksindstillinger", bliver ændret, før et system installeres på netværket.

14.3 Testdata

14.3.1 Sikring af testdata

Sikring af testdata
Data til test skal udvælges, kontrolleres og beskyttes omhyggeligt og i henhold til deres klassifikation.

15 Leverandørforhold

Det er vigtigt, at kommunen har overblik over og viden omkring dens leverandører for at sikre et tilfredsstillende sikkerhedsniveau. Leverandøren skal sikre, at underleverandørerne opfylder samme betingelser som leverandøren selv.

15.1 Informationssikkerhed i leverandørforhold

Mange aspekter af kommunens virke kan være omfattet af lovgivning eller påvirket af kontrakter eller eksterne parters rettigheder.

15.1.1 Informationssikkerhedspolitik for leverandørforhold

Vurdering og godkendelse af leverandør
Leverandøren skal kunne dokumentere et tilfredsstillende sikkerhedsniveau.

15.1.2 Netværksleverandør

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

15.2 Styring af leverandørydelser

15.2.1 Overvågning og gennemgang af leverandørydelser

Overvågning, kontrol og revision - Cloudløsning
Udbyderen skal kunne dokumentere, i hvilken grad aftalte servicemål er opfyldt.
Kommunen kan anmode om leverandørens dokumentation, IT-revisionsrapport, årlig risikovurdering eller tilsvarende.

15.2.2 Styring af ændringer af leverandørydelser

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

16 Styring af IT-sikkerhedsbrud

Konstaterede IT-sikkerhedsmæssige brud på eller trusler mod IT-sikkerheden skal registreres og dokumenteres, og alle væsentlige brud skal rapporteres til Chefen for Digitalisering & IT til vurdering samt til den løbende opsamling af sikkerhedsproblemer.
DPO'en skal underrettes ved IT-sikkerhedsmæssige brud der omhandler brud på persondatasikkerheden.

16.1 Styring af IT-sikkerhedsbrud og forbedringer

16.1.1 Ansvar og procedurer

Ansvar og forretningsgange for sikkerhedshændelser
Direktionen skal fastlægge forretningsgange der sikrer en hurtig, effektiv og metodisk håndtering af sikkerhedsbrud.

Proces for reaktion på hændelser
Den øverste sikkerhedsansvarlige har ansvar for at definere og koordinere en struktureret ledelsesproces, der sikrer en passende reaktion på sikkerhedshændelser.

Information om sikkerhedshændelser
Kommunen skal informere berørte parter internt og eksternt om eventuelle sikkerhedshændelser. Den øverste sikkerhedsansvarlige skal godkende alle eksterne meddelelser.

16.1.2 Rapportering af IT-sikkerhedshændelser

Rapportering af virusangreb
Hvis der observeres virus eller mistanke om virus, skal det omgående rapporteres til Digitalisering & IT.

16.1.3 Rapportering af IT-sikkerhedssvagheder

Rapportering af programfejl
Brugere der observerer programfejl skal rapportere dette til Digitalisering & IT.

Rapportering af formodede sikkerhedshændelser
Ved konstatering af eller mistanke om brud på IT-sikringsforanstaltninger skal dette straks rapporteres til den nærmeste chef og den ansvarlige direktør.

Rapportering af sikkerhedshændelser
Digitalisering & IT eller eventuelle outsourcingpartnere skal, når det er relevant, rapportere om hændelser af betydning for sikkerheden. Mere konkret skal fortrolighed, dataintegritet og tilgængelighed af systemer rapporteres.

16.1.4 Vurdering af og beslutning om IT-sikkerhedshændelser

Vurdering af tidligere hændelser
Mindst en gang om året skal Chefen for Digitalisering & IT gennemgå den forgangne periodes hændelser og på denne baggrund anbefale, hvorvidt IT-sikkerhedssystemet kan forbedres eller præciseres, f.eks. ved forslag om opdaterede regler, procedurer eller opdateret risikovurdering.

16.1.5 Håndtering af informationssikkerhedsbrud

Misligholdelse
Kommunen skal sikre, at systemet eller dele deraf kan afbrydes i tilfælde af misligholdelse, ved brud på sikkerheden, eller hvis løsningen indebærer en uacceptabel risiko for kommunens informationer og netværk.

16.1.6 Erfaring fra informationssikkerhedsbrud

Læring ved sikkerhedsbrud
Digitalisering & IT skal etablere en arbejdsgang, der kan registrere typer, omfanget og eventuelle omkostninger ved håndteringen af sikkerhedsbrud.

Kontrol og opfølgning på sikkerhedsbrud
Brud på sikkerheden, uautoriseret adgang og forsøg på uautoriseret adgang til systemer, informationer og data skal registreres.

16.1.7 Indsamling af beviser

Kontakt med relevante myndigheder
Ved brud på sikkerheden skal der være etableret en procedure for håndtering af bevismateriale og eventuelt kontakt med relevante myndigheder.

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.

17 IT-sikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Risikostyring og beredskabsplanlægning 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.

17.1 IT-sikkerhedskontinuitet

17.1.1 Planlægning af IT-sikkerhedskontinuitet

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

Beredskabsstyringsproces
Digitalisering & IT skal udarbejde og vedligeholde en tværorganisatorisk beredskabsplan, som skal behandle de krav til IT-sikkerhed, der er nødvendige for kommunens fortsatte drift.

Reetablering af systemer der er forretningskritiske på ny lokation

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

Identifikation af kritiske processer
Alle kritiske funktioner og disses relaterede processer, systemer og ejere skal være identificerede og dokumenterede.

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

Forsikring mod hændelser
Direktionen skal vurdere, om forsikring kan medvirke til minimering af risiko for tab. Især på områder, hvor sikringsforanstaltninger er vurderet som uhensigtsmæssige eller utilstrækkelige, skal dette overvejes.

17.1.2 Implementering af IT-sikkerhedskontinuitet

Beredskabsplaner for forretningskritiske funktioner
Systemejerne er ansvarlige for, at passende beredskabsplaner udarbejdes og vedligeholdes for de enkelte systemer med det formål at minimere nedbrud og udgifter som følge af sikkerhedshændelser.

Beredskabsplan
Beredskabsplan skal foreligge for alle forretningskritiske systemer

Aktivering af beredskabsplanen
Det skal være klart defineret, hvem der har ansvaret for aktivering af beredskabsplaner. Medarbejdere, der udgør en del af beredskabsplanen, skal være informeret om dette ansvar. Alle medarbejdere skal være informeret om beredskabsplanernes eksistens.

17.1.3 Verificer, gennemgå og evaluer IT-sikkerhedskontinuiteten

Uddannelse i beredskabsplaner
Systemejerne har ansvaret for, at der foregår tilstrækkelig uddannelse af medarbejdere i de aftalte beredskabsprocedurer, inklusive krisehåndtering.

Afprøvning og vedligeholdelse af beredskabsplaner
Beredskabsplaner skal løbende afprøves og opdateres for at sikre, at de er tidssvarende og effektive.

Afprøvning af beredskabsplaner skal indeholde
Test af nødprocedure (med henblik på at træne deltagerne i håndtering af deres roller efter episoden).

Opdatering af beredskabsplaner
Beredskabsplanen ajourføres løbende. Mindst 1 gang i hver valgperiode skal beredskabsplanen revideres.

18 Overensstemmelse

Mange aspekter af kommunens virke kan være omfattet af lovgivning eller påvirket af kontrakter eller eksterne rettigheder.

18.1 Overensstemmelse med lov- og kontraktkrav

18.1.2 Immaterielle rettigheder

Retningslinier for ophavsrettigheder

- Direktionen har det overordnede ansvar for, at kommunen fastholder en passende opmærksomhed på ikke at krænke tredjeparts ophavsrettigheder.
- Digitalisering & IT skal vedligeholde dokumentation for ejendomsretten af licenser, originalmateriale og manualer.
- Digitalisering & IT skal løbende kontrollere, at software-licensaftaler overholdes, f.eks. at eventuelle begrænsninger i antal brugere, servere eller kopier overholdes.
- Digitalisering & IT skal løbende kontrollere, at der kun er installeret autoriserede systemer med autoriserede licenser i kommunen.
- Brugere må ikke kopiere, konvertere eller udtrække information fra billed- og lydfiler eller tilsvarende ressourcer, medmindre dette specifikt tillades fra rettighedshaveren.
- Brugere må ikke, helt eller delvist, kopiere bøger, artikler, rapporter eller andre dokumenter medmindre dette specifikt tillades fra rettighedshaveren.

Administration af softwarelicenser

Registrering af software licenser sker gennem Digitalisering & IT. Det er Chefen for Digitalisering & ITs overordnede ansvar, at der er et tilstrækkeligt antal licenser til rådighed.
Medarbejdere må ikke forpligte kommunen ved at acceptere licensvilkår i software, som ikke er accepteret af Digitalisering & IT.

18.1.3 Beskyttelse af registreringer

Lovbestemte data

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

18.1.4 Privatlivets fred og beskyttelse af personoplysninger

EU-forordning (EU)2016/679

Europa-Parlamentets og Rådets forordning (EU)2016/679 af 27. april 2016 (Persondataforordningen) om beskyttelse af fysiske personer i forbindelse med enhver behandling af personoplysninger og om fri udveksling af sådanne oplysninger gælder for kommunen.

Opbevaring og behandling af personoplysninger

Lov om behandling af personoplysninger gælder ved enhver opbevaring og behandling af persondata.

Kontrol af overholdelse af persondatalovgivning

Den persondataansvarlige skal, i samarbejde med kommunens DPO, kontrollere overholdelse af Persondatafordningen.

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.

Dansk bekendtgørelse 528

Vejledning til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning gælder.

18.1.5 Regulering af kryptografi

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

18.2 Gennemgang af IT-sikkerhed

18.2.1 Uafhængig gennemgang af IT-sikkerhed

Gennemgang af sikkerhedspolitik
Den interne revision skal kontrollere at IT-sikkerhedspolitikken er indarbejdet i organisationen og overholdes. Kontrollen skal foretages mindst en gang årligt.

Opfølgning på implementering af sikkerhedspolitikken
Mindst hvert 2. år skal der udføres systematisk opfølgning på overholdelse af sikkerhedspolitikken i hele organisationen, og resultatet rapporteres til Direktionen.
Hver enkelt leder skal løbende sikre, at sikkerhedspolitikken bliver overholdt inden for eget ansvarsområde.

Dispensation for krav i sikkerhedspolitikken
Direktionen kan give dispensation for krav i sikkerhedspolitikken.

18.2.3 Undersøgelse af teknisk overensstemmelse

Sikkerhedstest af interne IT-systemer
Til brug ved revision skal der foreligge rapporter fra de seneste fire gennemførte sårbarhedsscanninger.