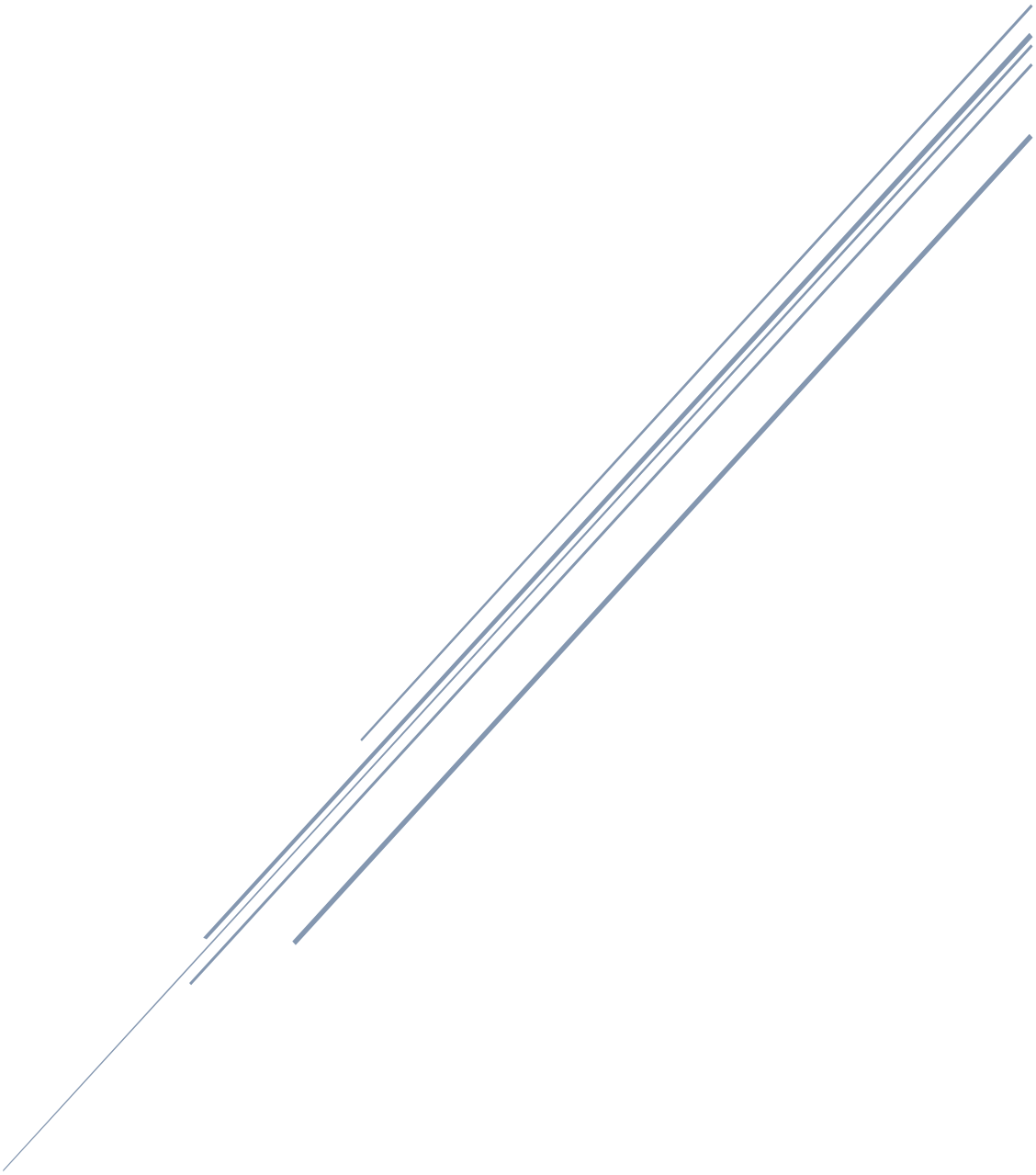
ALBERTSLUND KOMMUNE

Sikkerhedshåndbog 2018



ISO 27002:2013

Indhold

5 Informationssikkerhedspolitikker

5.1 Retningslinjer for styring af informationssikkerhed

5.1.1 Politikker for informationssikkerhed

Sprog for sikkerhedspolitik

It-sikkerhedspolitikken er udarbejdet på dansk og kun dansk.

Omfang af informationssikkerhedspolitik

Informationssikkerhedspolitikken er en integreret del af den overordnede it-sikkerhedspolitik .
Informationssikkerhed defineres som de samlede foranstaltninger til at sikre fortrolighed, tilgængelighed og integritet. Foranstaltninger inkluderer tekniske, proceduremæssige, regel- og lovmæssige kontroller.

Publicering af sikkerhedspolitik

Informationssikkerhedspolitikken skal offentliggøres og kommunikeres til alle relevante interessenter, herunder alle medarbejdere.
Kommunens it-sikkerhedspolitikker består af en overordnet sikkerhedspolitik.

5.1.2 Gennemgang af politikker for informationssikkerhed

Vedligeholdelse af sikkerhedspolitik

Sikkerhedspolitikken vedligeholdes af Albertslund Kommunes Økonomi & Stab (ØS)

Revision af sikkerhedspolitik

Der skal ske en revision af sikkerhedspolitikken mindst en gang om året eller ved væsentlige ændringer.

Revision af den overordnede it-sikkerhedspolitik

Der skal ske en revision af den overordnede it-sikkerhedspolitik mindst hvert femte år samt ved væsentlige ændringer.

Vedligeholdelse af sikkerhedspolitik

Det er den it-sikkerhedsansvarlige, der er på vegne af kommunaldirektøren, har det overordnede ansvar for, at organisationen udarbejder sikkerhedspolitikker, regler, procedurer og tilhørende dokumentation.

Godkendelse af sikkerhedspolitik

Sikkerhedspolitikken skal godkendes af direktionen.

6 Organisering af informationssikkerhed

6.1 Intern organisering

6.1.1 Roller og ansvarsområder for informationssikkerhed

Sikkerhedsorganisation

Albertslund Kommune skal have et forum for informationssikkerhed, der har ansvar for at sikre, at strategien for informationssikkerhed er synlig, koordineret og i overensstemmelse med virksomhedens mål.

Topledelsens rolle

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

Ejerskab

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.

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

Sikkerhedsansvar for systemer og programmer

Sikkerhedsansvarlige systemejere for virksomhedskritiske systemer (centerchefer) skal identificeres og gøres opmærksom på dette ansvar. Disse ejere skal have ansvar og beføjelser til at sikre tilstrækkelig beskyttelse.

Ejerskab

I Albertslund Kommune er det afdelingschefen, der er ansvarlig for systemer, som primært bruges i egen afdeling. Hvis et system bruges i mere end et center, så er det afdelingschefen i det center, som er den primære bruger, som er systemejer. Afdelingschefen for øvrige brugere af systemet er ansvarlig for de autorisationer, som er givet til brugerne i eget center.

ØS er ansvarlig for de systemer, som går på tværs af hele kommunen (ESDH, økonomi, Office pakke) med samme ansvar for alle brugere uanset afdelingstilknytning.

Den enkelte afdelingschef er dog stadig ansvarlig for de autorisationer, som er givet den enkelte medarbejder i eget afdeling.

Ansvar for adgangsrettigheder

Systemejeren har ansvaret for at fastlægge og løbende revurdere adgangsrettigheder i overensstemmelse med kommunens generelle adgangspolitik.

Opfølgning på implementering af sikkerhedspolitikken

Hver enkelt leder skal løbende sikre, at sikkerhedspolitikken bliver overholdt inden for eget ansvarsområde.

6.1.2 Funktionsadskillelse

Sikring af forretningskritiske systemer

Forretningskritiske systemer skal sikres gennem etableringen af brugerprofiler for at hindre misbrug af disse. For at mindske risikoen for misbrug af privilegier, skal alle systemer beskyttes ved hjælp af funktionsadskillelse.

Funktionsadskillelse: udvikling, test og driftsmiljøer

Der er ingen krav til funktionsadskillelse i forbindelse med udviklings-, test- og driftsmiljøet.

6.1.3 Kontakt med myndigheder

Samarbejde med tilsynsmyndigheden for personoplysninger

AK 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.

Kontakt med relevante myndigheder

Ved brud på sikkerheden skal der være etableret en procedure for håndtering af bevismateriale og eventuelt kontakt med relevante myndigheder.
Hvis personoplysninger kompromitteres, skal den it-sikkerhedsansvarlige meddele dette til tilsynsmyndigheden inden for 72 timer eller formelt retfærdiggøre forsinkelser ud over de 72 timer.
Hvis tredjepart behandler personoplysninger, skal denne underrette den it-sikkerhedsansvarlige, hvis et brud på persondatasikkerheden er opstået.

6.1.4 Kontakt med særlige interessegrupper

Information om nye trusler, virus og sårbarheder

Økonomi & Stab skal holde sig orienteret inden for de benyttede platforme.

Økonomi & Stab skal informere relevante personer i ledelsen om nye trusler, som potentielt kan berøre de pågældende forretningsenheder.

Økonomi & Stab er ansvarlig for eksternt samarbejde med de fornødne informationskanaler, herunder samarbejde omkring it-sikkerhed med relevante eksterne interessegrupper og sikkerhedsorganisationer.

Økonomi & Stab skal etablere en proces for identifikation af nye sårbarheder. Der skal udpeges en ansvarlig person eller gruppe for dette.

Kontakt med interessegrupper og fora

Økonomi & Stab skal oparbejde og vedligeholde kontakt med sikkerhedsfaglige interessegrupper.

6.1.5 Informationssikkerhed ved projektstyring

Projektmodellen skal indeholde følgende overvejelser omkring informationssikkerhed:

- Kravspecifikationen skal indeholde kravene til informationssikkerhed.
- Identifikation af nødvendige sikringstiltag skal blandt andet gøres ved hjælp af risikovurderinger
- Informationssikkerhed bør være en integreret del af projektledelse.

6.2 Mobilt udstyr og fjernarbejdspladser

6.2.1 Politik for mobilt udstyr

Mobile enheders tilslutning til andre netværk

Det er tilladt at forbinde mobilt udstyr til andre netværk.

Fortrolige data på mobile enheder

Der må opbevares fortrolige data på mobile enheder, såfremt disse data beskyttes med et sikkerhedsprodukt, der er godkendt af IT.

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, diske, USB-nøgler, cd'er, dvd'er m.v.

Arbejdsmobil (uden multimediebeskatning)

Må kun benyttes til arbejdsrelaterede formål.

Beskeder på mobilsvarer skal aflyttes og behandles.

Fritelefon

Ved fri telefon forstås, at abonnementet enten er oprettet i Albertslund Kommunes navn som ejer, og med medarbejderens navn som bruger. bærer en direkte risiko for telefonregningens størrelse.

Må benyttes til private formål, dog ikke til konkurrencedeltagelse samt bidrag til velgørende formål. Må benyttes i udlandet i begrænset omfang.

Beskeder på mobilsvarer skal aflyttes og arbejdsmæssige henvendelser behandles.

PDA (i hjemmeplejen)

Må kun benyttes til arbejdsrelaterede formål.

Brug af fastnettelefon

Alle organisationsenheder skal sikre at der udarbejdes lokale retningslinjer, så det sikres at telefonerne besvares i åbningstiden.

6.2.2 Fjernarbejdspladser

Sikring af medarbejderes fjernarbejdspladser og deres kommunikationsforbindelser skal beskyttes i forhold til de informationer og forretningssystemer, de benyttes til.

Adgang fra distancearbejdspladser

Kun Albertslund Kommunes IT-udstyr må få direkte adgang. Øvrigt privat og offentligt tilgængeligt IT-udstyr i internet caféer m.v. må således ikke få direkte adgang.

Adgang gives kun for brugere, der er autentificerede med brugernavn og kodeord.

Krav til sikring af udstyr uden for Albertslund Kommunes overvågning

Udstyr, der benyttes uden for Albertslund Kommunes lokaliteter, skal beskyttes efter samme retningslinjer, som gælder for udstyr, der benyttes inden for Albertslund Kommunes lokaliteter under hensyntagen til de særlige risici ved ekstern anvendelse.

7 Personalesikkerhed

7.1 Før ansættelsen

7.1.1 Screening

Baggrundscheck af ansatte

Vedkommendes chef skal efter vurdering tilse, at der sker forsvarligt baggrundscheck af medarbejdere med ansvar for forretningskritiske arbejdsområder.

Baggrundscheck af medarbejdere kan omfatte

En personlig reference.

Ansøgerens curriculum vitæ.

Uddannelser og professionelle kvalifikationer.

Verifikation af referencer

Udvalgte referencer eller eksamensbeviser for betroede medarbejdere skal verificeres. HR og Personale vurderer individuelt nødvendigt omfang af verifikation.

Ren straffeattest

Der skal følges procedure for indhentelse og anvendelse af straffeattester i AK for nyansatte.

Baggrundscheck af konsulenter

Den ansvarlige chef, der indgår aftale med en ekstern konsulent
skal tilse, at der sker forsvarligt baggrundscheck af konsulenten.

Tavsheds-/fortrolighedserklæring ved ansættelse

Alle medarbejdere skal som en del af ansættelseskontrakten underskrive en tavshedserklæring. Alle ansættelsesmyndigheder SKAL senest ved ansættelsestidspunktet sørge for, at tavshedserklæringen underskrives.

7.1.2 Ansættelsesvilkår og -betingelser

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

Tavsheds-/fortrolighedserklæring ved ansættelse

Alle medarbejdere skal som en del af ansættelseskontrakten underskrive en tavshedserklæring. Alle ansættelsesmyndigheder SKAL senest ved ansættelsestidspunktet sørge for, at tavshedserklæringen underskrives.

Ansvar for sikkerhed

I stillings- og funktionsbeskrivelser for medarbejdere med adgang til forretningskritiske data og systemer skal sikkerhed indgå i beskrivelsen.

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 Albertslund Kommunes systemer og data.
- er gjort bekendt med de vedtagne retningslinier, så de kan leve op til virksomhedens informationssikkerhedspolitik.
- holder sig inden for de retningslinier og bestemmelser, der er for ansættelsen, inkl. Albertslund Kommunes informationssikkerhedspolitik og konkrete arbejdsmetoder.

Det er tillige ledelsens ansvar at centret er tilstrækkeligt bemandet for at løse de sikkerhedsopgaver som følger af lovgivningen og de vedtagne sikkerhedspolitikker

7.2.2 Bevidsthed om, uddannelse og træning i informationssikkerhed

Uddannelse i sikkerhedspolitikken Medarbejdere i Økonomi & Stab

- Medarbejdere i IT og digitalisering har et særligt ansvar for at tilegne sig reglerne i lovgivningen omkring sikkerhed.

Medarbejdere i Albertslund Kommune

- Alle medarbejdere skal løbende holde sig a jour med kommunens sikkerhedsregler og politikker via intranetttet.
- Alle medarbejdere modtager løbende instruktioner i overholdelse af virksomhedens informationssikkerhedspolitik.

7.2.3 Sanktioner

Overtrædelse af sikkerheds retningslinjerne

Alle overtrædelser af sikerhedsretningslinjerne skal indberettes til Økomomi & Stab uden ugrundet ophold. Økomomi & Stab rapporterer hændelsen til øverste ledelse straks, samtidig med at relevant afdelingschef underrettes, såfremt det ikke allerede er sket.
Overtrædelse af sikkerhedspolitikken kan medføre ansættelsesretslige konsekvenser, i form af enten påtale, irettesættelse, advarsel, afskedigelse eller bortvisning. Det er ledelsen i samråd med HR og Økomomi & Stab, der vurderer i den enkelte, konkrete situation.

- Det er ikke tilladt at foretage uautoriseret afprøvning af sikkerheden.
- Det er ikke tilladt at forsøge at omgå sikkerhedsmekanismer.

Test af sikkerheden er alene et Økomomi & Stab anliggende.

7.3 Ansættelsesforholdets ophør eller ændring

7.3.1 Ansættelsesforholdets ophør eller ændring

Fortrolighedserklæring og fratrædelse

I henhold til ansættelsesbrevet, ophører tavshedspligten hverken ved ændring i funktion eller ved fratrædelse.

8 Styring af aktiver

8.1 Ansvar for aktiver

8.1.1 Fortegnelse over aktiver

Registrering af it-udstyr

Der skal vedligeholdes en fortegnelse over samtlige relevante enheder, som er forbundet til virksomhedens it- infrastruktur.

Administration af internet-domænenavne

Der skal forefindes en liste over kommunens registrerede domænenavne, status for brug, betalingsoplysninger og dato for fornyelse. Listen varetages af Økomomi & Stab.

8.1.2 Ejerskab af aktiver

Sikkerhedsansvar for informationsaktiver

ØS har ansvar for vedligeholdelse af en liste over samtlige informationssystemer i Kommunernes IT OverbliksSystem (KITOS). Listen skal angive henholdsvis den sikkerhedsansvarlige data- og systemejer for hvert enkelt system.

8.1.3 Accepteret brug af aktiver

Kryptering af privat udstyr

Der er særlige krav til kryptering af private udstyr. Ved overførsel af informationer til/fra privat udstyr skal ØS sikre, at der anvendes samme krypteringsteknologi som til virksomhedens øvrige udstyr.

Brugere af sociale netværk skal være specielt opmærksomme på at:

Det er tilladt at bruge sociale netværk, og det kan være en god kommunikationsform til relevante drøftelser mellem kolleger og vidensleverandører som f.eks. KL og andre. Privat brug af sociale netværk bør begrænses til pauser.

Det er et ledelsesmæssigt ansvar, at brugen af sociale netværk ikke har indflydelse på det konkrete arbejde. Browsere på kommunens pc'er gemmer blandt andet information om brug af sociale netværk, og kommunen kan få adgang til denne information.

Kommunens sikkerhedskopier kan indeholde data om din brug af it generelt, herunder din brug af sociale netværk.

De sociale netværk, som du bruger, kan registrere og gemme oplysninger om dig og hvilke informationer, du søger og bruger.

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

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

Persondata må aldrig deles på sociale netværk.

Brug af cloud services

Det er ikke tilladt at dele, eller lagre virksomhedens informationer i 'skyen', ved brug af cloud serviceudbydere som eksempelvis Dropbox, Google mfl.

Albertslund Kommune anvender Microsoft OneDrive, men alle personfølsomme data skal gemmes i ESDH eller i det relevante fagsystem.

Der skal gennemføres en risikovurdering, hvor de it-sikkerhedsmæsige trusler som er forbundet med cloud- løsningen, vurderes, inden aftaler indgås.

Medarbejderes private brug af e-mail

Det er acceptabelt at benytte e-mail til private beskeder i rimeligt og begrænset omfang.

Medarbejderne må anvende mailsystemerne til personligt brug i begrænset omfang, hvis dette ikke har indflydelse på virksomhedens drift og sikkerhed i øvrigt. Al mailtrafik betragtes som virksomhedens ejendom. Virksomheden forbeholder sig ret til at skaffe sig adgang til data og e-mail for medarbejdere, hvis dette sker af drifts- eller sikkerhedshensyn. Virksomheden vil så vidt muligt forsøge at undgå at åbne eventuel privat e-mail- korrespondance.

Brug af mobile enheder

Albertslund Kommune anvender i videst muligt omfang bærbart eller mobilt udstyr. Udstyret skal medbringes som håndbagage under rejser.

8.1.4 Tilbagelevering af aktiver

Returnering af aktiver ved aftrædelse

Medarbejderen skal returnere samtlige informationsaktiver, der tilhører virksomheden, på sin sidste arbejdsdag.

8.2 Klassifikation af information

8.2.1 Klassifikation af information

Informationer og data skal klassificeres som følger:

Offentligt: Materiale, der frit må udleveres til offentligheden.
Virksomhedskritisk: Informationer, der er vigtige for kerneområdet i forretningen. Høj tilgængelighed og stor integritet er kritisk, uanset hvilket fortrolighedsniveau, der i øvrigt kræves.
Eksternt brug: Materiale, der frit må udleveres til eksterne parter uden at fortrolighedsaftaler kræves.
Personhenførbart: Data er relateret til et individ, f.eks. en kunde, en borger, en patient eller en medarbejder.

Ansvar for klassifikation

Det er systemejer, som har ansvaret for, at aktivet er klassificeret.

8.2.2 Mærkning af information

8.2.3 Håndtering af aktiver

Tyveri eller bortkomst af mobilt udstyr

Medarbejderen har pligt til at opbevare udstyr, der anvendes til behandling af virksomhedens informationer, på forsvarlig vis.

Økomomi & Stab skal kontaktes straks, i tilfælde af tyveri/bortkomst af enheden.

Økomomi & Stab skal sikre, at informationer på bortkommet mobilt udstyr kan slettes (wipes).

8.3 Mediehåndtering

8.3.1 Styring af bærbare medier

Opbevaring og registrering af datamedier

Systemejer skal sikre, at medierne eller informationerne på mediet klassificeres, og at brugere er instrueret i at opbevare mediet i henhold til regler for klassifikationen.

8.3.2 Bortskaffelse af medier

Bortskaffelse og genbrug af medier

Alle datamedier, f.eks. harddiske, USB-nøgler, Memorycards, dvd'er, cd'er og bånd skal sikkerhedsslettes eller destrueres inden bortskaffelse.

Destruktionsmetoden skal være effektiv og ske ved enten makulering, afbrænding, opstrimling eller lignende. Økomomi & Stab håndterer alle datamedier i forbindelse med destruktion. Alle bærbare og stationære skal derfor indleveres til Økomomi & Stab forinden de bortskaffes.

Beholdere med papirmateriale til destruktion skal holdes aflåste.

8.3.3 Fysiske medier under transport

Brug af mobile enheder

Bærbart udstyr skal medbringes som håndbagage på rejser. Kommunens udstyr bør kun undtagelsesvis medbringes på ferier til udlandet.

9 Adgangsstyring

9.1 Forretningsmæssige krav til adgangsstyring

9.1.1 Politik for adgangsstyring

Brugeradministration, outsourcing leverandør

Leverandøren skal følge virksomhedens regler for brugerstyring.

Begrænset adgang til informationer

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

Inddragelse af brugerrettigheder ved fratrædelse

Der skal forefindes en opdateret procedure for inddragelse af privilegier i forbindelse med fratræden eller afskedigelse af personale.

Sikkerhedsmedarbejdere kan rekvirere en liste over fratrådte medarbejdere for de seneste seks måneder fra HR.

Tildeling af brugerrettigheder

Den systemansvarlige for et it-system bestemmer nødvendige brugerrettigheder for systemet. Sikkerhedsmedarbejderen skal kvalificere de pågældende rettigheder.

Retningslinjer for adgangsstyring

Økomomi & Stab har ansvar for at etablere og vedligeholde procedurer for kommunens adgangs- og rettighedsstyring. Systemejere har ansvar for at etablere og vedligeholde procedurer for deres systemers adgangs- og rettighedstyring.

Adgangsbegrænsning til informationer

Applikationer skal sikre, at adgang til informationer sker efter en veldefineret adgangspolitik.

Identifikation af brugerprofiler for eksterne brugere

Eksterne brugerprofiler skal, gennem konsistent navngivning, være tydeligt adskilt fra fastansatte medarbejderes brugerprofiler. Bruger-ID skal udarbejdes efter en standard-navnekonvention. Dette gælder også for gæster, konsulenter og lignende således, at disse let kan identificeres.

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

Fratrædelse

Når ansættelse eller midlertidige kontrakter ophæves, skal alle tilknyttede rettigheder trækkes tilbage. ID-kort og lignende skal afleveres, og it-udstyr skal inddrages ved fratrædelsen.

9.1.2 Adgang til netværk og netværkstjenester

Forbindelse til fremmede trådløse netværk

Brugere må forbinde sig til fremmede trådløse netværk.

Styring af netværksadgang

Adgangskontrolsystemet skal som standard være konfigureret til at blokere al anden adgang end den, som er specifikt tilladt.

Økomomi & Stab skal ved styring af brugernes netværksadgang sikre imod uautoriseret anvendelse af fælles netværk og hertil knyttede tjenester.

Adgang til applikationer på virksomhedens netværk

Der gives kun adgang til applikationer på internt netværk, som er sikkerhedsgodkendt.

Adgang til trådløse netværk

Brugere skal autentificeres, ved hjælp af et certifikat, før der gives adgang til andre dele af kommunens trådløse netværk end gæstenetværket.

Overvågning af netværk

Økomomi & Stab skal årligt udføre evalueringer af regler for netværkstrafik i firewalls og routere.

Autentificering ved fjernadgang til netværket

Fjernadgang til det interne netværk skal beskyttes ved hjælp af VPN med individuelle certifikater. To-faktor autentifikation skal benyttes ved fjernadgang til det interne netværk.

Hvis integration af informationssystemer resulterer i en forøget risiko, skal denne vurderes og godkendes af Økomomi & Stab.

Information til eksterne partnere

Relevante interessenter skal informeres om krav til efterlevelse af sikkerhedspolitikkerne i kommunen.

Outsourcing-partnere

Alle outsourcing-partnere skal bekræfte kendskab til kommunens sikkerhedspolitik.

Ekstern revision af outsourcing-partnere

Outsourcing-partnere som behandler personhenførbare data skal sørge for ekstern revision mindst en gang om året. Alle databehandlere skal udfylde en databehandleraftale som skal foreligge i kommunen og som skal opdateres årligt.

9.2 Administration af brugeradgang

9.2.1 Brugerregistrering og -afmelding

Identifikation og autentifikation af brugere

Alle brugere skal have en unik identitet til personlig brug.

Der skal benyttes en passende autentifikationsteknik til verifikation af brugernes identitet. Brugeridentiteten skal kunne spores til den person, som er ansvarlig for en given aktivitet. Fælles brugeridentiteter for en gruppe brugere eller en specifik opgave kan benyttes, hvis det er forretningsmæssigt forsvarligt.

Brugen af en fælles brugeridentitet skal godkendes af centerledelsen.

Gennemgang af brugerprofiler

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

9.2.2 Tildeling af brugeradgang

Registrering af brugere

Systemejer skal autorisere brugeradgang.

Økomomi & Stab vedligeholder vejledninger og skabeloner for, hvordan bruger-ID eller rettigheder fjernes eller ændres ved ophør eller ændring af brugeres jobfunktion.

Der skal ske en verifikation af, at rettighedsniveauet er i overensstemmelse virksomhedens generelle sikkerhedsretningslinier.

Serviceleverandørerer skal anvende tilsvarende eller samme autorisationsprocedure som virksomheden.

Processerne for tildeling af adgangsrettigheder skal indeholde:

- Kontrol af, om de ønskede adgangsrettigheder er i overensstemmelse med virksomhedens kommercielle behov.
- Hvordan brugere eller brugerrettigheder fjernes eller ændres ved ophør af eller ændringer i brugeres jobfunktioner.
- Kontrol af, om de ønskede adgangsrettigheder på nogen måde er i strid med kravet om funktionsadskillelse.
- Kontrol af, om adgangsrettigheder er i overensstemmelse med klassificeringen af oplysningerne.
- Kontroller der sikrer, at der ikke sker brud på relevant lovgivning og kontrakter ved disse adgangsrettigheder.

Medarbejderes omplacering

Ved ændringer af roller for medarbejderne skal brugerrettigheder revurderes.

9.2.3 Styring af privilegerede adgangsrettigheder

Skift af administratoradgangskode ved fratrædelse

Hvis en person med kendskab til administrative adgangskoder fratræder, skal disse adgangskoder ændres med det samme.

Tildeling af brugerrettigheder

Systemejer for et it-system bestemmer nødvendige brugerrettigheder for systemet.

Økomomi & Stab bestemmer og tildeler brugerrettigheder på virksomhedens tværgående it-systemer.

Registrering af brugere

Brugere skal have unikt brugernavn og bruger-ID.

Systemejer skal autorisere brugeradgang.

Adgangsrettigheder skal afstemmes med de forretningsmæssige behov.

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

Serviceleverandørerer skal anvende tilsvarende eller samme autorisationsprocedure som kommunen. Kommunen skal vedligeholde fortegnelser over, hvordan brugere eller brugeres rettigheder fjernes eller ændres ved ophør eller ændring af brugeres jobfunktion.

Udvidede adgangsrettigheder

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

De udvidede adgangsrettigheder må ikke sættes i kraft, før den fornødne autorisation er indhentet. Automatiserede systemtekniske processer skal anvendes i videst muligt omfang for at begrænse behovet for tildeling af udvidede rettigheder.

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

Der skal benyttes særlige brugeridentiteter til de udvidede rettigheder hos netværks administratorer.

Dette af hensyn til overvågning og opfølgning.

Ændring af administrative adgangskoder

Administrator adgangskoder skal ændres hvert kvartal.

Administrator adgangskoder skal følge samme minimumsregler som øvrige adgangskoder.

Administrator adgangskoder skal ændres hvis udenforstående får kendskab til disse, herunder hvis administratorer forlader kommunen.

9.2.4 Styring af autentifikationsinformation om brugere

Identifikation af brugerprofiler for eksterne brugere

Eksterne brugerprofiler skal, gennem konsistent navngivning, være tydeligt adskilt fra fastansatte medarbejderes brugerprofiler.

Bruger-ID skal udarbejdes efter en standard-navnekonvention. Dette gælder også for gæster, konsulenter og lignende således, at disse let kan identificeres.

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

Sikkerhedsvurdering af tredjepart

Der skal udføres en sikkerhedsvurdering (f.eks. i form af revisions rapport, virksomhedens egen udtalelse af IT-sikkerhed) af tredjepart før et eventuelt samarbejde.

Sikkerhed ved samarbejde med partnere

Ved integration af kommunens systemer og processer med tredjepart skal sikkerhedsrisici altid vurderes og dokumenteres.

Integration af informationssystemer

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

Lagring af adgangskoder

Adgangskoder til kritiske systemer må aldrig lagres elektronisk i klartekst.

Retningslinjer for adgangskoder

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

Ved ændring af adgangskoden til fagsystemer og netværks login afsendes email til brugeren om, at adgangskoden er ændret. Midlertidige adgangskoder til netværket må oplyses telefonisk, alle andre password sendes via email.

9.3 Brugernes ansvar

9.3.1 Brug af autentifikationsinformation

Valg af sikre adgangskoder

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

Lagring af adgangskoder

Adgangskoder må aldrig lagres elektronisk i klartekst.

Krav til indhold og længde af adgangskode

Adgangskoder skal indeholde mindst 8 tegn, hvoraf mindst to skal være tal.

Krav til indhold af adgangskode

Adgangskoder skal indeholde kombinationer fra mindst tre af følgende kategorier: store bogstaver, små bogstaver, tal og specialtegn.
(æ, ø og å må ikke anvendes)

Genbrug af adgangskode

Medarbejderne må ikke anvende samme adgangskode til infrastrukturen som til adgang til tredjeparts udstyr, f.eks. internet-websteder og netbanker. Omfattende brug af samme adgangskode på tredjepart systemer øger sandsynligheden for, at adgangskodens fortrolighed krænkes.

Det er brugerens ansvar at vælge en tilstrækkeligt sikker adgangskode.

Krav til skift af adgangskode

Adgangskoder skal skiftes efter højst 90 dage.

Brug af autologin funktioner

Automatiseret log-in til systemer og applikationer må ikke anvendes.

Adgangskoder er strengt personlige

Adgangskoder er strengt personlige og må ikke deles med andre.

Retningslinjer for brug af netværkstjenester

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

9.4 Styring af system- og applikationsadgang

9.4.1 Begrænset adgang til informationer

Adgang til produktionsdata

Systemadministratorers adgang til fortrolige oplysninger skal begrænses.

Adgang til funktionalitet og data i forretningssystemer

Informationssystemer skal overholde virksomhedens adgangskontrolpolitik.

Politikken for adgangskontrol på de enkelte systemer skal baseres på en risikovurdering og på de forretningsmæssige behov.

9.4.2 Procedurer for sikker log-on

Sikker log-on

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

Automatiske afbrydelser

Funktioner i et informationsbehandlingssystem, der ikke har været aktivt i et fastlagt tidsrum, skal automatisk afbrydes.

9.4.3 System for administration af adgangskoder

Systemer til styring af adgangskoder

Adgangskontrolsystemet skal låse en brugerkonto i 30 minutter, hvis brugeren har overskredet det tilladte antal af adgangsforsøg.
Adgangskontrolsystemet skal låse brugerkonti efter fem forgæves adgangsforsøg.

Så vidt muligt skal der benyttes it-systemer, der automatisk kan styre de krav, der findes til adgangskoder.

9.4.4 Brug af privilegerede systemprogrammer

Brug af systemværktøjer

Økomomi & Stab skal begrænse og styre adgangen til systemværktøjer, f.eks. utilities, der kan påvirke eller omgå systemers eller enheders sikkerhed.
Systemansvarlige og sikkerhedsmedarbejdere er autoriserede til at anvende systemværktøjer i begrænset omfang og altid under instruks fra ØS. Dette gælder også outsourcingleverandør.

9.4.5 Styring af adgang til kildekoder til programmer

Kontrolleret adgang til kildekode

Kildekode må ikke opbevares i driftsmiljøet.

Der skal indhentes tilladelse til opdateringer af kildebiblioteker og tilhørende dokumentation.

Kildekode og bibliotekerne med denne skal sikres.

Vedligeholdelse og kopiering af kildekode skal følge en dokumenteret procedure for ændringsstyring. Alle adgange til kildebibliotekerne skal logges.

10 Kryptografi

10.1 Kryptografiske kontroller

10.1.1 Politik for anvendelse af kryptografi

Kryptering af filer

Filer må ikke krypteres på det interne netværk. Personfølsomme data som sendes ud af kommunens netværk skal krypteres.

Godkendte krypteringsprodukter

Økonomi & Stab skal vedligeholde en liste over godkendte krypteringsløsninger.

Fortrolige data på mobile enheder

Der må opbevares fortrolige data på mobile enheder, såfremt disse data beskyttes med et produkt, der er godkendt af Økonomi & Stab.

Kryptering af administrative netværksforbindelser

Forbindelser der benyttes til it-administration, skal krypteres, hvis de benytter offentlige eller usikre netværk, f.eks. internettet.

Brug af kryptering i forbindelse med opbevaring af data
Fortrolige informationer skal altid være krypteret, når de opbevares på transportabelt udstyr, f.eks. på bærbare computer, håndholdte computere m.m.

11 Fysisk sikring og miljøsikring

11.1 Sikre områder

11.1.1 Fysisk perimetersikring

Overvågning i sikre områder
Borgere må ikke få adgang til sikre zoner.

Overvågning i sikre områder
Økonomi & Stab skal sikre, at arbejde i sikre områder så vidt muligt overvåges.

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

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

Indbrudsalarmer
Kommunen skal anvende passende alarmsystemer på relevante bygninger og lokaler.

11.1.2 Fysisk adgangskontrol

Adgangskort til håndværkere og andet midlertidigt personale
Håndværkere, reparatører, teknikere og andre gæster, der får udleveret midlertidige adgangskort, skal bære disse synligt.

Adgangskort og nøglebrikker
Adgangskontrolkort og nøglebrikker er personlige. De skal opbevares forsvarligt og må ikke overdrages til tredjepart.

11.1.3 Beskyttelse mod eksterne og miljømæssige trusler

Brandsikring

Serverrum må ikke benyttes som lager for brændbare materialer. Serverrum skal sikres med veldimensioneret brandslukningsudstyr.

11.1.4 Arbejde i sikre områder

Aflåsning af lokaler og bygninger

Alle døre og vinduer skal kunne låses forsvarligt.

11.1.5 Områder til af- og pålæsning

Af- og pålæsningsområder

Af- og pålæsningsområder skal indrettes, så risiko for uautoriseret adgang til virksomhedens øvrige områder mindskes. Adgang til af- og pålæsningsområder må kun gives til identificerede og autoriserede personer.

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 ØS.

Spisning og rygning i nærheden af udstyr

Der må ikke ryges, spises eller drikkes i serverrum eller i nærheden af forretningskritisk udstyr.

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 teknikum

Alle krydsfelter og andre teknikum skal
være aflåste.

11.2.2 Understøttende forsyninger (forsyningssikkerhed)

Køling

Serverrum og hovedkrydsfelt skal sikres med veldimensionerede airconditionanlæg.

Nødstrømsanlæg

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

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.

11.2.4 Vedligeholdelse af udstyr

Vedligeholdelse af udstyr og anlæg

ØS er ansvarlig for reparationer og forbyggende vedligeholdelse.

Kun godkendte leverandører må udføre reparationer og vedligeholdelse. ØS skal godkende alle leverandører, der skal udføre reparationer på kommunens udstyr. Pc'ere repareres og vedligeholdes af godkendt reparatør på stedet, så enhederne ikke forlader kommunen.

11.2.5 Fjernelse af aktiver

Fjernelse af udstyr fra virksomheden

Udstyr må kun fjernes fra virksomheden, hvis der foreligger en underskrevet kvittering på det udleverede.

11.2.6 Sikring af udstyr og aktiver uden for organisationen

Opsyn med mobile enheder

Mobile enheder må ikke efterlades synligt i f.eks. bilen.

Adgang til data på bærbare pc'er skal beskyttes med en login-adgangskode. Udstyr må ikke indeholde personfølsomme informationer uden at der er anvendt harddisk-kryptering.

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. Det er altid ØS, der træffer beslutning om brugt udstyr.

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 placeres så informationerne ikke kan ses af uvedkommende.

11.2.9 Politik for ryddeligt skrivebord og blank skærm

Brug af adgangskodebeskyttet pauseskærm

Adgangskodebeskyttet skærmlås skal aktiveres på pc-arbejdspladser når man forlader sin plads i mere end 3-4 minutter.

Opbevaring af fysiske dokumenter

Skriveborde skal ryddes for fortrolige dokumenter senest ved arbejdsdagens afslutning.

Dokumenter med personhenførbare oplysninger skal opbevares i aflåst skab eller skuffe efter arbejdstid.

Fortrolige dokumenter skal opbevares i aflåst skab eller skuffe.

Udskrivning

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

12 Driftssikkerhed

12.1 Driftsprocedurer og ansvarsområder

12.1.1 Dokumenterede driftsprocedurer

Sikring af arbejdsstationer inden ibrugtagning

Alle arbejdsstationer skal installeres ved brug af den, af ØS, fastlagte procedure.

Alle arbejdsstationer skal sikres inden brug. Minimum sikring inkluderer installation af seneste sikkerhedsrettelser for operativsystemet og antivirus-program.

Driftsansvar

ØS er sammen med den valgte driftsleverandør ansvarlig for drift og administration af fælles it-systemer samt disses sikkerhed. Dette inkluderer efterlevelse af sikkerhedspolitikker, regler og procedurer.

Sikkerhed i systemplanlægning

Ved planlægning af systemer skal sikkerhedsbetragtninger altid medtages i overvejelserne.
Konfigurationsstandarder for samtlige systemkomponenter skal kunne håndtere alle kendte sårbarheder og være overensstemmende med branche-accepterede standarder for hærdning af systemer.
It-sikkerhedskrav skal tages i betragtning ved design, aftestning, implementering og opgradering af it-systemer samt ved systemændringer.

Driftsafviklingsprocedurer

ØS skal gennem den valgte driftsleverandør for forretningskritiske systemer have dokumenterede, ajourførte og tilgængelige procedurer tilgængelig for driftsafviklingspersonalet og andre med et arbejdsbetinget behov.
Operationelle procedurer skal indeholde installationen, konfiguration af systemer samt en beskrivelse af, hvordan databehandling håndteres manuelt og automatiseret (services og batch jobs).
Operationelle procedurer skal omfatte krav til og konfiguration af backup, job-schedulering, sikkerhedskonfigurationer og instruktioner til håndtering af fejl.
Driftsprocedurer skal omfatte beskrivelser af genopretnings- og retableringsprocedurer samt konfiguration af overvågnings-og revisionsspor.

Sikring af serversystemer

Kommunen skal sikre at den valgte driftsleverandør har hærdet alle servere gennem deaktivering af unødvendige og usikre services og protokoller.
Alle systemkomponenter skal hærdes gennem deaktivering eller fjernelse af unødvendige funktioner (f.eks. scripts, drivere, underliggende filsystemer og webservere).

Registrering af driftsstatus

ØS er ansvarlig for at identificere, logge og håndtere hændelser og afvigelser i driften af de it-systemer, de er ansvarlige for.

ØS skal registrere væsentlige forstyrrelser og uregelmæssigheder i driften af systemerne samt årsager hertil. Dette skal ske gennem den valgte driftsleverandør.

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.
Der skal indhentes en formel godkendelse af ændringen, før arbejdet med den går i gang. System ansvarlige skal acceptere ændringer, før de implementeres i produktions miljøet. 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 ikke forstyrrer de involverede forretningsydelser.
ØS skal sikre at den valgte drifsleverandør opretter og vedligeholder procedurer for ændringsstyring for alle software- og systemkonfigurationsændringer (inklusiv netværksudstyr).
Der skal foretages test af driftsfunktionaliteten, før ændringer gennemføres.

Retningslinjer for ændringer

ØS har ansvaret for, at driftsleverandøren dokumenterer en entydig identifikation og registrering af væsentlige ændringer.
ØS har ansvaret for, at driftsleverandøren dokumenterer en nødprocedure til at mindske effekten af fejlslagne ændringer.

12.1.3 Kapacitetsstyring

Kapacitetsplanlægning

It-systemernes dimensionering skal afpasses efter kapacitetskrav. Belastning skal overvåges, så opgradering og tilpasning kan finde sted løbende. Dette gælder især for virksomhedskritiske systemer. Den valgte driftsleverandør skal overvåge at der er tilstrækkelig kapacitet for at sikre pålidelig drift indenfor rammerne af den indgåede kontrakt. Afvigelser skal rapporteres som hændelser til ØS.

12.1.4 Adskillelse af udviklings test- og driftsmiljøer

Sikring af applikationsudviklingsmiljøerne

Udviklings og testmiljøer skal sikres mod trusler som uautoriseret adgang, ændringer og tab. Disse skal så vidt mulligt være adskilt fra driftsmiljøer. Data skal sikres efter følsomhedsniveau.

12.2 Beskyttelse mod malware

12.2.1 Kontroller mod malware

Antivirusprogrammer

Antivirus-programmer skal installeres på alle mobile enheder og fjernarbejdspladser. Programmerne skal opdateres dagligt.

Antivirus-produkter på systemer

ØS sikrer, at der er installeret aktive antivirus-produkter på samtlige computere i virksomheden, og at disse opdateres højst et døgn efter leverandørens opdateringer.

Der skal etableres foranstaltninger til at sikre mod vira, orme, trojanske heste mv. Dette indebærer, at der skal indføres procedurer for personalet til at håndtere disse.

Der skal udføres en regelmæssig scanning og gennemgang af malwarebeskyttede systemer for at sikre, at alle systemer er beskyttet og har opdaterede signaturfiler

Malware scanning skal undersøge filer modtaget over netværk eller via en hvilken som helst form for lagringsmedie, vedhæftede filer i e-mails og downloads, servere samt relevante endpoints såsom bærbare computere og arbejdsstationer.

Kontrol af antivirus på arbejdsstationer

Medarbejdere kan antage, at antivirus fungerer. Det er alene ØSs ansvar at kontrollere korrekt funktion.

Spam-mail beskyttelse

AK bortfiltrerer e-mail inkl. eventuelle vedhæftede filer, der opfylder Albertslund 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.

12.3 Backup

12.3.1 Backup af information

Opbevaring af sikkerhedskopier på ekstern lokation

Den fysiske sikkerhed på den eksterne opbevarings-lokalitet skal sikres gennem besigtigelse mindst en gang årligt.

Reserveanlæg og -udstyr samt datamedier med sikkerhedskopier skal opbevares i sikker afstand for at undgå skadevirkninger fra et uheld på det primære anlæg.

Backup af systemer og data

ØS er ansvarlig for sikker lagring og backup af data på serverudstyr. Dette sker gennem den valgte driftsleverandør.

Backup skal være nøjagtig, fuldstændig og omfatte dokumenterede restore-procedurer

Overvågning af procedurer for sikkerhedskopiering

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

Nødplaner for sikkerhedskopiering

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

12.4 Logning og overvågning

12.4.1 Hændelseslogning

Opfølgningslogning

ØS sørger gennem den valgte driftsleverandør at

- logge sikkerhedshændelser på virksomhedens væsentlige systemer
- der foretages logning af al adgang til systemkomponenter (inklusive netværksudstyr)
- logge fejlhændelser på virksomhedens væsentlige systemer
- logge væsentlige brugeraktiviteter på virksomhedens systemer

- logge fejlhændelser på virksomhedens systemer
- logge sikkerhedshændelser på kommunens systemer

Opbevaring af opfølgningslog

ØS skal opbevare

- log for fejlhændelser på væsentlige system i mindst 3 måneder
- log for sikkerhedshændelser på væsentligesystem i mindst 3 måneder
- log for brugerhændelser på væsentlige system i mindst 3 måneder
- logregistreringer i minst et år. Logregistreringerne skal være tilgængelige on line i mindst 3 måneder.

Hændelseslogning

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

Alle sikkerhedshændelser skal logges og indberettes til ØS som opbevarer i en fastlagt periode af hensyn til opfølgning på adgangskontroller og eventuel efterforskning af fejl og misbrug.
Alle medarbejdere, samarbejdspartnere og øvrige brugere skal være bekendt med forretningsgangene for rapportering af forskellige typer hændelser og svagheder, der kan have indflydelse på sikkerheden for kommunens aktiver. Sikkerhedshændelser og svagheder skal hurtigst muligt rapporteres til IT.

Overvågning af internet-brug

Den enkelte medarbejders anvendelse af internettet bliver logget og kan anvendes hvis anvendelsen strider mod kommunens principper for anvendelse af internettet.

Fejllog

Fejl skal logges og analyseres, og nødvendige udbedringer og modforholdsregler skal gennemføres.

12.4.2 Beskyttelse af logoplysninger

Beskyttelse af log-oplysninger

Kun personer, hvis arbejde kræver dette, må tillades adgang til logs.

12.4.3 Administrator- og operatørlog

Administrator-log

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

Overvågning af systemleverandøren

Systemejerne skal mindst halvårligt overvåge serviceleverandørerne, gennemgå de aftalte rapporter og logninger samt udføre egentlige revisioner for at sikre, at aftalen overholdes, og at sikkerhedshændelser og - problemer håndteres på betryggende vis.

Overvågning af driftsleverandøren

ØS skal regelmæssigt overvåge drifts og serviceleverandørerne, gennemgå de aftalte rapporter og logninger samt udføre egentlige revisioner for at sikre, at aftalen overholdes, og at sikkerhedshændelser og -problemer håndteres på betryggende vis.

12.5 Styring af driftssoftware

12.5.1 Softwareinstallation på driftssoftware

Krav til indstillinger af internet-browser

MS Internet Explorer og andre browsere skal opsættes af ØS, jævnfør sikkerhedspolitikken. Brugerne må ikke ændre denne opsætning.

Installation af programmer på arbejdsstationer

Operativsystemer og applikationer må kun installeres og ændres af ØS på godkendt udstyr. Anvendelsen af ikke-godkendt udstyr m.v. vil resultere i disciplinære sanktioner.

Softwareopdateringer generelt

Systemejere skal holde sig informeret om alle programrettelser til programmer, der anvendes i centret og hurtigst muligt give ØS besked på at installere disse på alle computere. ØS vurderer, hvornår rettelserne har positiv indflydelse på den samlede sikkerhed.
ØS forestår installation af alle større programrettelser, når det vurderes, at disse har positiv indflydelse på den samlede sikkerhed. Det sker i samarbejde med den valgte system og driftsleverandør.

12.6 Sårbarhedsstyring

12.6.1 Styring af tekniske sårbarheder

Større programpakkeopdateringer f.eks. "service packs"

Når større opdateringer f.eks. service packs er gjort tilgængelige fra leverandører, skal ØS sammen med

den valgte driftsleverandør vurdere, om disse skal installeres.
Større opdateringer skal testes i et testmiljø, inden opdateringerne installeres i produktionsmiljøet.

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

Sikkerhedsopdateringer til netværksudstyr

ØS skal sørge for, at alle benyttede trådløse adgangspunkter og software til disse er opdateret med de seneste sikkerhedsrettelser. Dette sker gennem den valgte driftsleverandør. Udrulning/installation skal foretages senest 30 dage efter udgivelsen af sikkerhedsrettelsen.

Rettelser til applikations-programpakker

Systemejer skal løbende vurdere tilgængelige sikkerhedsrettelser f.eks. patches eller hot-fixes. Udrulning/installation skal foretages efter behov.
ØS forestår installation af alle større programrettelser, når det vurderes, at disse har positiv indflydelse på den samlede sikkerhed. Det sker i samarbejde med den valgte system og driftsleverandør.

Styring af antivirus

ØS skal kunne styre antivirus på alle systemer centralt. Med styring menes overvågning af, om alle antivirus- programmer er aktivt kørende, tvungen opdatering, scanning, oprydning og generering af opfølgningslog.

Rettelser til operativsystemer

ØS skal løbende vurdere tilgængelige sikkerhedsrettelser, f.eks. patches eller hot-fixes til anvendte operativsystemer. Udrulning/installation skal foretages efter behov.

ØS forestår installation af alle større programrettelser, når det vurderes, at disse har positiv indflydelse på den samlede sikkerhedAlle ændringer i forretningskritiske systemer skal udføres efter godkendt procedure. Alle procedurer skal indeholde en alternativ plan til retablering af det forretningskritiske system. Vilkårene for aktivering af den alternative plan skal ligeledes fremgå af proceduren.
Det sker i samarbejde med den valgte system og driftsleverandør.

Ændringer i forretningskritiske systemer

Alle ændringer i forretningskritiske systemer skal udføres efter godkendt procedure. Alle procedurer skal indeholde en alternativ plan til retablaring af det forretningskritiske system. Vilkårene for aktivering af den alternative plan skal ligeledes fregå af proceduren.

12.6.2 Begrænsninger på softwareinstallation

Administration af softwarelicenser

Registrering af software licenser sker gennem ØS. Det er its overordnede ansvar, at der er et tilstrækkeligt antal licenser.

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

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

Sikring af netværk

ØS har det overordnede ansvar for at beskytte kommunens netværk.

Placering af trådløse netværk

Udstyr til trådløst netværk bør placeres svært tilgængeligt og må kun forbindes til den eksisterende infrastruktur af ØS .

Adgang til trådløse netværk for gæster

Gæster, hvis identitet er kendt, må tilslutte sig til gæstenettet.

Gæster, hvis identitet er kendt, må tilslutte eget udstyr til gæstenettet, forudsat at udstyret ikke generer andre systemer.

Adgang til aktive netværksstik

Adgang til aktive netværksstik styres af ØS.

Adgang til netværket

Adgang til kommunens netværk må kun ske gennem sikkerhedsgodkendte løsninger.

Adgang til data på kommunens netværk

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

Adgang til applikationer på kommunens netværk

Der gives kun adgang til applikationer på internt netværk, som er godkendt af ØS.

Opbevaring af fortrolige informationer på privat udstyr

Der må ikke behandles eller opbevares personhenførbare eller personfølsomme informationer på udstyr, der ikke tilhører kommunen.

Indkommende netværksforbindelser

Der tillades kun etablering af forbindelser fra internet til interne servere efter godkendelse af ØS.

Installation af netværksudstyr

Netværksadgang kontrolleres og styres af ØS. Kun nødvendige adgange må være aktive infrastrukturen. Alle øvrige skal være lukket ned.
Netværksstik i offentligt tilgængelige områder, må kun aktiveres, når dette er forretningsmæssigt begrundet. Ved tilslutning af udstyr til netværksstik i offentligt tilgængelige områder, tillades tildeling af ip-adresser ved hjælp af DHCP.

Installation af netværksudstyr til trådløs adgang

Medarbejderne må ikke installere netværksudstyr som for eksempel routere, access points, der giver trådløs adgang til udstyr som tablets og bærbare pc'ere. Dette kan kun ske gennem ØS.

Krav til firewall

For at kunne opdage og undgå web-baserede angreb, skal der installeres en applikations-firewall foran alle applikationer, der kan tilgås fra internettet.
Firewallen må kun tillade protokoller og trafik som er forretningsmæssigt begrundet.

Der skal opsættes en firewall mellem den demilitariserede netværkszone (DMZ) og internettet. Firewallen skal blokere al ind- og udgående trafik, som ikke er specifikt tilladt.

Sikring af netværk

ØS har det overordnede ansvar for at beskytte virksomhedens netværk.

Tilslutning af udstyr til netværk

Det er ikke tilladt, at ansatte kobler udstyr til netværket. Udstyret kan forstyrre driften.

Adgang til netværket

Adgangen til virksomhedens netværk må kun ske gennem sikkerhedsgodkendte løsninger.

Adgang til aktive netværksstik

Adgang til aktive netværksstik skal styres af ØS.

Netværksstik i offentligt tilgængelige områder, må kun aktiveres, når dette er forretningsmæssigt begrundet.

Begrænset netværkstid

Brugersystemer med særlig høj risiko skal kræve fornyet autentifikation med fastlagte intervaller.

Fysisk sikring af netværk

Krydsfelter og kabeltermineringer skal være placeret så fysisk adgang begrænses.

Udgående netværksforbindelser

Det er kun tilladt at tilgå services på internet og andre netværk via godkendte proxy-servere.

Netværksdokumentation

Netværksdiagrammet skal

- omfatte samtlige trådløse netværks
- indeholde en beskrivelse den logiske administration
- være opdateret

ØS følger op på den valgte driftsleverandør.

13.1.2 Sikring af netværkstjenester

Fjernstyring og administration

Forbindelser til fjernadgang til brug for leverandører og support, skal overvåges, mens de benyttes.

Afvikling af programmer i forbindelse med internetsurfing

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

Internetbaserede tjenester

Det er tilladt at bruge internettjenester, der ikke er beskrevet i sikkerhedspolitikken, såfremt dette ikke indebærer forøgede sikkerhedsrisici.

Brug af kryptering i forbindelse med dataudvikling

Adgangskoder skal sendes krypteret.

13.1.3 Opdeling af netværk

Opdeling af netværk

ØS skal sammen med den valgte driftsleverandør segmentere netværk for at etablere en passende adskillelse imellem forskellige tjenester, brugergrupper eller systemer.
Mindstekrav til netværkssegmentering er, at der etableres 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

Udlevering af fortrolige informationer og oplysninger

Fortrolig information må ikke udleveres uden forudgående aftale med dokument- eller dataejer. Personhenførbare og fortrolige oplysninger må kun udleveres til bemyndigede personer. Fortrolig information må ikke videregives til tredjepart i nogen form, uden godkendelse af dette fra informationsejeren. Dette gælder især for følsom information, samt personhenførbare oplysninger givet til organisationen.

Elektroniske dokumenter

Elektroniske kopier af dokumenter, f.eks. indscannede dokumenter og faxer, med fortrolige eller følsomme informationer, må kun behandles og lagres på passende it-udstyr.

13.2.3 Elektroniske meddelelser

Ejerskab

Virksomheden betragter alle e-mails som virksomhedens ejendom.

Opbevaring og sletning af e-mail

E-mail, der indeholder personhenførbare oplysninger, skal behandles i overensstemmelse med persondataloven og databeskyttelsesforordning/GDPR (30 dage).

Autentificering

Alle brugere skal anvende virksomhedens interne bruger-autentificering. Ved intern kommunikation har brugerne dermed vished for modpartens autenticitet.

Elektronisk udveksling af post og dokumenter

Hvis e-mail bruges til bindende aftaler, skal de underskrives med en digital signatur.

Fortrolig mail

E-mail med følsomt indhold skal krypteres med godkendt software. Dette gælder især for klassificeret, fortrolig eller følsom persondata, der sendes over internettet.

Social Engineering

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

Vedhæftede filer

ØS skal blokere for filtyper som kommunen vurderer farlige eller uhensigtsmæssige.

Phishing og bedrageri (awareness)

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

Sagsbehandling og journalisering af e-mail

Sendte og modtagne e-mails skal håndteres på same måde som traditionel post og fax. E-mails med vigtig information skal journaliseres systematisk for at sikre dokumentation og lagring.

Anvendelse af sociale netværk

Sociale netværk må gerne anvendes fra kommunens it-systemer.

Kommunens informationer på sociale netværk

Kommunens informationer må aldrig deles på et socialt netværk (overvej derfor altid hvad du skriver). Brugere af sociale netværk skal være specielt opmærksomme på at:

- Personer på sociale netværk er ikke altid dem de udgiver sig for at være
- Persondata må aldrig deles på sociale netværk
- Download af filer som du modtager via et socialt netværk er underlagt de samme regler som øvrige downloads
- Informationer som du har lagt ud på et socialt netværk, kan kun meget vanskeligt, måske aldrig, trækkes tilbage
- Du vil med stor sandsynlighed opleve at nogen forsøger at franarre dig dine bruger-id''er og/eller dine adgangskoder (phishing).
- De sociale netværk, du bruger, kan registrere og gemme oplysninger om dig og hvilke informationer du søger og bruger.

Medarbejderes private brug af e-mail

Medarbejderne må anvende mailsystemerne til personligt brug i begrænset omfang, hvis dette ikke har indflydelse på kommunens drift og sikkerhed i øvrigt. Al mailtrafik betragtes som kommunens ejendom. Kommunen forbeholder sig ret til at skaffe sig adgang til data og e-mail for medarbejdere, hvis dette sker

af drifts- eller sikkerhedshensyn. Kommunen vil så vidt muligt forsøge at undgå at åbne eventuel privat e-mailkorrespondance.

Download af filer fra internettet

Filer må downloades fra internettet i begrænset arbejdsmæssigt omfang under hensyntagen til den daglige itdrift.

Download af programmer fra internettet

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

Streaming via internet

Det er ikke tilladt at anvende kommunens netværk til tung og vedvarende trafik, som eksempelvis tv-tjenester eller film, medmindre det er fagligt relevant.

Terminalsessioner til fjernstyring

Godkendt personale må tilgå visse virksomhedssystemer over internet forbindelser, hvis disse sikres på forsvarlig vis. Adgang skal tillades af systemejer og gives af ØS.

Medarbejderes private brug af internetadgang

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

Brug af preview-funktion til åbning af e-mail

E-mail må gerne vises i preview-funktion.

Automatisk indholdsfiltrering

Systemerne skal jævnligt scannes for spam- og phishing-mails. 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.

14 Anskaffelse, udvikling og vedligeholdelse af systemer

14.1 Sikkerhedskrav til informationssystemer

14.1.2 Analyse og specifikation af informationssikkerhedskrav

Anskaffelsesprocedurer

Det skal sikres, at nyanskaffelser ikke giver anledning til konflikt med eksisterende krav i sikkerhedspolitikken. Anskaffelser må ikke give anledning til forøget risiko for sikkerhedshændelser uden forudgående risikovurdering og eventuel detaljeret risikoanalyse.
Ethvert nyt system skal risikovurderes inden ibrugtagning.

Anskaffelse og installation af nye programmer og systemer skal igennem en godkendelsesprocedure.

14.1.2 Sikring af applikationstjenester på offentlige netværk

Offentlig tilgængelig information

Det er driftsleverandørens ansvar, at offentlig tilgængelig information, f.eks. på kommunens web-server(e), er passende beskyttet mod uautoriserede ændringer.

14.1.3 Beskyttelse af handelsapplikationer og -tjenester

Foranstaltninger ved e-handel skal omfatte:

- Krav til beskyttelse af fortrolighed og integritet for ordreoplysninger
- Procedurer for tildeling af autorisationer til at indgå bindende købs- og salgsaftaler
- Krav til fortrolighed og integritet for alle købsordrer, betalingsoplysninger, leveringsadresser og kvitteringer
- Procedurer for verifikation af autorisationer
- Krav til fortrolighed for følsomme oplysninger
- Kontrolprocedure for betalingsoplysninger
- Krav til kontrol af autenticitet af både køber og sælger
- Krav til en sikker og hensigtsmæssig betalingsprocedure
- Beskyttelse mod tab eller gentagelse af transaktioner

14.2 Sikkerhed i udviklings- og hjælpeprocesser

14.2.1 Sikker udviklingspolitik

Sikkerhed i applikationsudvikling

Udviklingsprocessen skal dokumenteres.

Softwareudvikling skal baseres på best practice og indbefatte informationssikkerhed gennem hele softwareudviklingens livscyklus.
Sikkerhed skal inkluderes som en integreret del af alle udviklingsprojekter.

Validering af inddata

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

Kontrol af intern databehandling

Systemejer skal sikre en kontrol af datas korrekthed i kommunens systemer eller applikationer med det formål at afsløre, om data kan være eller er blevet modificeret, enten på grund af systemfejl eller bevidste handlinger.

Validering af uddata

Uddata fra kommunens systemer med økonomisk konsekvens valideres løbende med det formål at sikre, at data så vidt muligt er korrekte.

14.2.2 Procedurer for styring af systemændringer

Migreringsstyring

Planlægning, test og godkendelse af ændringer:

- Ændringer skal planlægges og afprøves inden de sættes i drift.
- Ændringernes konsekvenser skal vurderes inden drift.
- Ændringer skal igennem en formaliseret godkendelsesprocedure inden drift.

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.

Ændringer i driftsmiljøerne skal annonceres i god tid således, at der er god tid til gennemgang og test inden implementeringen.

Beredskabsplanerne skal tilrettes i overensstemmelse med nye ændringer.

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.

Indbyggede sikringstiltag, f.eks. logning samt adgangs- og integritetskontrol, bør gennemgås for at sikre, at de ikke er kompromitterede.

14.2.5 Principper for udvikling af sikre systemer

Sikkerhedskrav til informationsbehandlingssystemer

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

Sikkerhed i systemplanlægning

Ved planlægning af systemer skal sikkerhedsbetragtninger altid medtages i overvejelserne.

It-sikkerhedskrav skal tages i betragtning ved design, aftestning, implementering og opgradering af it-systemer samt ved systemændringer.

Specifikation af sikkerhedskrav

Sikkerhedskrav skal være dokumenteret i forbindelse med enhver it-system-nyanskaffelse eller it-systemopgradering. Dette gælder både for kundetilpassede- og standardsystemer.

14.2.6 Sikkert udviklingsmiljø

Sikring af udviklingsmiljøer

Ved risikovurdering af systemudvikling bør følgende overvejes:

- Omfanget af følsomme 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, hvis det foretages decentralt
- 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

14.2.7 Outsourcet udvikling

Systemudvikling udført af ekstern leverandør

- AK kræver løbende dokumenteret kvalitetssikring
- AK kræver ophavsrettighed på kildekode
- Aftaler om accepttest for kvalitet, nøjagtighed og sikkerhed skal identificeres og være en del af leverancer. Leverandøren skal desuden være i stand til at validere effektiviteten af udviklingsprocesserne.

Ejerskab af data, cloudløsninger

Virksomheden skal sikre, at ejerskab, herunder regler for ophavsret, kildekode mm. er klart defineret mellem virksomheden og cloududbyder.

Ekstern revision af outsourcing-partnere

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

14.2.8 Systemsikkerhedstest

Test af sikkerhedsfunktioner

Sikkerhedstests skal gennemføres i forbindelse med udviklingsprocessen.Testen skal udføres efter aftale

i det konkrete udviklingsprojekt.

14.2.9 Systemgodkendelsestest

Godkendelse af nye eller ændrede systemer

ØS skal etablere en godkendelsesprocedure for nye systemer, for nye versioner og for opdateringer af eksisterende systemer samt de afprøvninger, der skal foretages, inden de kan godkendes og sættes i drift. Godkendelsesproceduren skal sikre, at standardværdier, eksempelvis standard administrator-logins og andre "fabriksindstillinger", bliver ændret, før et system installeres på netværket.
Systemaccepttest bør altid tage højde for relevante sikkerhedskrav for blandt andet automatiseret kodetest og sårbarhedstest.

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. Det skal formelt godkendes, inden data fra driftsmiljøet kopieres til et testmiljø. Data fra driftsmiljøet, der anvendes i testmiljøer, skal slettes omgående efter afsluttet test.

15 Leverandørforhold

15.1 Informationssikkerhed i leverandørforhold

15.1.1 Informationssikkerhedspolitik for leverandørforhold

Vurdering og godkendelse af outsourcing leverandør

ØS skal deltage i vurdering og godkendelse af outsourcingleverandører.

Leverandøren skal kunne dokumentere et tilfredsstillende sikkerhedsniveau. Leverandøren skal kunne dokumentere sit sikkerhedsniveau eksempelvis i form af revisorerklæring, intern auditrapport eller it-revisionsrapport.

Anskaffelse, udvikling og vedligeholdelse ved outsourcing

Leverandøren skal have passende formelle procedurer baseret på best practices på området (change- og patch management-procedurer).

15.1.2 Håndtering af sikkerhed i leverandøraftaler

Håndtering af sikkerhed i procedurer for leverandøraftaler

Relevante sikkerhedskrav skal identificeres og aftales med leverandører, der har adgang til, behandler, opbevarer eller leverer it-infrastruktur til organisationens informationsaktiver
Kravene indeholder:

- Beskrivelse af de relevante informationsaktiver
- Tilpasning af organisationens og leverandørers klassifikationssystemer
- Identifikation af lovkrav, såsom regler for databeskyttelse, ophavsret, intellektuel ejendomsret og overholdelse af industrikrav
- Sikkerhedskrav for logisk og fysisk adgang
- Retten til at udføre revision
- Leverandørens forpligtelse til at være i overensstemmelse med kommunens sikkerhedspolitikker
- Awareness- og uddannelsesprogrammer.

Misligholdelse, cloudløsning

AK skal sikre, at servicen hos en valgt driftsleverandør kan afbrydes i tilfælde af misligholdelse, ved brud på sikkerheden, eller hvis løsningen indebærer en uacceptabel risiko for kommunens informationer og netværk.

AK skal have en "exit-strategi" på plads i tilfælde af misligholdelse.

15.1.3 Forsyningskæde for informations- og kommunikationsteknologi

Netværkssikkerhed, outsourcing leverandør

Den valgte driftsleverandør skal sikre en hensigtsmæssig opbygning af netværk, firewall, segmentering, kryptering mm. Vurdering kan ske på baggrund af sårbarhedsvurdering, it-revisorerklæring eller leverandørens interne auditrapport. Leverandøren skal foretage periodiske test af netværk og firewall, fx. penetrationstest.
Disse kan udføres af tredjepart.

Leverandøren skal kunne levere:

De nødvendige

- tekniske opsætninger til at sikre opkoblinger i overensstemmelse med samarbejdsaftalen
- sikkerhedsniveau i hele leverandør-forsyningskæden

15.2 Styring af leverandørydelser

15.2.1 Overvågning og gennemgang af leverandørydelser

Overvågning af serviceleverandør

ØS skal regelmæssigt overvåge serviceleverandørerne, ved at gennemgå de af de systemejende centre aftalte og indhentede rapporter og logninger samt udføre egentlige revisioner for at sikre, at aftalen overholdes, og at sikkerhedshændelser og -problemer håndteres på betryggende vis.

15.2.2 Styring af ændringer af leverandørydelser

Styring af ændringer hos serviceleverandøren

ØS skal sammen med det relevante center sikre, at ændringsstyring af serviceleverandørens ydelser følger samme retningslinier som virksomhedens egne.

16 Styring af informationssikkerhedsbrud

16.1 Styring af informationssikkerhedsbrud og forbedringer

16.1.1 Ansvar og procedurer

Ansvar og forretningsgange for sikkerhedshændelser

Ledelsens skal placere ansvar for at fastlægge forretningsgange, der sikrer en hurtig, effektiv og metodisk håndtering af sikkerhedsbrud. Sikkerhedsbrud håndteres centralt i ØS.
Ved et konstateret sikkerhedsbrud tager den konkrete person straks fat i sin centerchef enten via mail eller via telefon, og samtidig orienteres ØS, som herefter tager fat på en undersøgelse.
ØS rapporterer til alle relevante myndigheder ligesom rapportering sker til Økonomiudvalg / Byråd på førstkommende møde. I særlige tilfælde laves en orientering til alle byråds medlemmer, som sendes af borgmesteren.

Information om sikkerhedshændelser

AK skal inden 72 timer på faktuel vis informere berørte parter internt og eksternt om eventuelle sikkerhedshændelser. Kommunaldirektøren skal godkende alle eksterne meddelelser.

Proces for reaktion på hændelser

Der skal etableres en proces, som sikrer at hændelsesstyringsplanen løbende evalueres og tilpasses i overensstemmelse med indsamlet erfaring og den generelle udvikling inden for industrien.
AK skal sikre, at personale med ansvar for at reagere på sikkerhedsbrister, uddannes i tilstækkeligt omfang. Hændelsesstyringsplanen

- skal indgå i sammenhæng med og henvise til beredskabsplaner og retableringsprocedurer
- skal testes mindst en gang om året
- skal indeholde kommunikations- og kontaktstrategier
- sikre, at ansvarligt personale er tilgængeligt og kan reagere på sikkerhedsbrister døgnet rundt

Den sikkerhedsansvarlige har ansvar for at definere og koordinere en struktureret ledelsesproces, der sikrer en passende reaktion på sikkerhedshændelser, og skal definere telefonnumre, e-mail-adresser og elektroniske formularer til indrapportering af sikkerhedshændelser.

16.1.2 Rapportering af informationssikkerhedshændelser

Sikkerhedshændelser hos outsourcing leverandør

Leverandøren registrerer sikkerhedshændelser, f.eks. brud på fortrolighed, tilgængelighed eller integritet, i eget system. Leverandøren skal straks og uden ugrundet ophold underrette ØS på et foruddefineret telefonnummer, hvis der sker en sikkerhedshændelse, f.eks. ved brud på fortrolighed, integritet eller tilgængelighed.

Rapportering af sikkerhedshændelser

Organisationen og eksterne tjenesteudbydere er forpligtede til at indberette enhver observeret sikkerhedshændelse eller mistanke herom. Der bør være let adgang til rapportering af disse hændelser. Alle sikkerhedshændelser skal dokumenteres og revideres mindst en gang om året.

Rapportering af formodede sikkerhedshændelser

Ved konstatering af brud eller formodede brud på it-sikringsforanstaltninger skal rapportering straks ske til egen centerchef og ØS.
Årsager til sikkerhedshændelser kan være:

- Ineffektive sikringstiltag
- Brud på fortrolighed, integritet og tilgængelighed
- Menneskelige fejl
- Brud på fysisk sikkerhed
- Manglende efterlevelse af politikker eller procedurer
- Brud på logisk adgang
- Malware, virus eller hacking
- Driftsforstyrrelser (systemændringer, hardwarefejl mm.)

Sikkerhedshændelser ved brug af privat udstyr

AK kan afbryde for adgangen til privat udstyr i tilfælde af sikkerhedsbrud, misligholdelse eller hvis det vurderes at udstyret udgør en uacceptabel risiko for virksomhedens informationer og netværk.

Rapportering af virusangreb

Hvis der observeres virus eller mistanke om virus, skal det omgående rapporteres til driftsleverandøren.

16.1.4 Vurdering af og beslutning om informationssikkerhedshændelser

Vurdering af tidligere hændelser

For at kunne mindske sandsynligheden eller effekten af fremtidige sikkerhedshændelser, skal den forgangne periodes hændelser gennemgås mindst en gang om året.

16.1.5 Håndtering af informationssikkerhedsbrud

Kontrol og opfølgning på sikkerhedsbrud

Brud på sikkerheden, uautoriseret adgang og forsøg på uautoriseret adgang til systemer, informationer og data skal registreres.
Sikkerhedsbrud såsom uautoriserede forsøg på adgang til systemer, netværk eller data skal logges.
Reaktionsprocessen for sikkerhedshændelser bør omfatte:

- indsamling af beviser
- efterforskning
- sikring af, at alle aktiviteter er korrekt logget for efterfølgende analyse og gyldige som bevismateriale
- Efterfølgende analyse af hændelsen

16.1.6 Erfaring fra informationssikkerhedsbrud

At lære af sikkerhedsnedbrud

ØS etablerer et system, der følger op på de sikkerhedsbrud der har været i den forløbne periode og hvilke tiltag der i fremtiden skal foretages for at imødekomme fremtidige sikkerhedsbrud. Tiltag forelægges direktionen til beslutning.

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 - skal der indsamles, opbevares og præsenteres et fyldestgørende bevismateriale. ØS har ansvaret for kontakten til myndighederne og det relevante center, som indsamler data sammen med den relevante driftsleverandør.

17 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

17.1 Informationssikkerhedskontinuitet

17.1.1 Planlægning af informationssikkerhedskontinuitet

Ramme for beredskabsplaner

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

Beredskabsstyringsproces

ØS skal udarbejde og vedligeholde en tværorganisatorisk beredskabsstyringsproces, som skal behandle de krav til informationssikkerhed, der er nødvendige for virksomhedens fortsatte drift.

17.1.2 Implementering af informationssikkerhedskontinuitet

Beredskabsplan

Beredskabsplan skal foreligge for alle forretningskritiske systemer

Beredskabsplaner for virksomhedskritiske 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.

Aktivering af beredskabsplanen

Det skal være klart defineret, hvem der har ansvaret for aktivering af beredskabsplaner. Alle medarbejdere skal være informeret om beredskabsplanernes eksistens.

Nødplaner for sikkerhedskopiering

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

17.1.3 Verificer, gennemgå og evaluer informationssikkerhedskontinuiteten

Afprøvning og vedligeholdelse af beredskabsplaner

Beredskabsplaner skal løbende afprøves og opdateres for at sikre, at de er tidssvarende og effektive. Det konkrete center er ansvarlig for at planerne afprøves.

Afprøvning af beredskabsplaner skal indeholde:

- Teknisk retablering (sikring af at tekniske systemer kan retableres effektivt).
- En skrivebordstest af de forskellige scenarier.

Uddannelse i beredskabsplaner

ØS og det konkrete center har ansvaret for, at der foregår tilstrækkelig uddannelse af medarbejdere i de aftalte beredskabsprocedurer, inklusive krisehåndtering.

18 Overensstemmelse

18.1 Overensstemmelse med lov- og kontraktkrav

18.1.1 Identifikation af gældende lovgivning og kontraktkrav

Opbevaring og behandling af personoplysninger

Lov om behandling af personoplysninger gælder ved enhver opbevaring og behandling af persondata. Der må ikke behandles personoplysninger af fortrolig karakter på privat pc. Personoplysninger af fortrolig karakter må ikke opbevares eller behandles på bærbar pc, medmindre kryptering anvendes og bekendtgørelse nr. 528 om personoplysninger overholdes.

18.1.2 Immaterielle rettigheder

Identifikation af relevante patenter

Ledelsen er ansvarlig for, at patenter, der influerer på virksomhedens drift, identificeres.

Retningslinjer for ophavsrettigheder

Kommunens øverste ledelse har det overordnede ansvar for, at kommunen fastholder en passende opmærksomhed på ikke at krænke tredjeparts ophavsrettigheder.
Systemansvarlige skal

- vedligeholde dokumentation for ejendomsretten af licenser
- løbende kontrollere, at software-licensaftaler overholdes, f.eks. at eventuelle begrænsninger i antal brugere, servere eller kopier overholdes.

Brugere må ikke

- kopiere, konvertere eller udtrække information fra billed- og lydfiler eller tilsvarende ressourcer, medmindre dette specifikt tillades fra rettighedshaveren
- helt eller delvist, kopiere bøger, artikler, rapporter eller andre dokumenter medmindre dette specifikt tillades fra rettighedshaveren

Rettigheder kan f.eks. opnås gennem CopyDan eller andre.

18.1.3 Beskyttelse af registreringer

Lagring og adgangsrettigheder til systemdokumentation

Systemdokumentation opbevares i mindst 3 år.

Lovregulerede data

Virksomheden skal beskytte lovregulerede data mod ændring, sletning, samt uautoriseret adgang.

Sikring af virksomhedens lovbestemte data

Virksomhedens 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

Personoplysninger må kun behandles i henhold til gældende lov, og kun hvis de er indsamlet til et specifikt formål og behandles nøjagtigt og sikkert

Virksomheden skal sikre at personoplysninger behandles loyalt, lovligt og på en gennemsigtig måde for den registrerede

Personoplysninger skal være relevante, tilstrækkelige og må kun bruges til det fastsatte formål.
Personoplysninger må ikke opbevares længere end nødvendigt.

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.

Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden

AK skal senest 72 timer efter et brud på persondatasikkerheden, foretage anmeldelse til tilsynsmyndigheden. 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.

Ret til indsigt i personoplysninger

Den registrerede har til enhver tid ret til, at anmode virksomheden om at få indsigt i hvilke personoplysninger der behandles om vedkommende.

18.1.5 Regulering af kryptografi

Regulering på kryptografiområdet

Ansvaret for overholdelse af regulativer og brug af kryptografiske produkter påhviler systemejer for de systemer, hvorpå disse implementeres.

18.2 Gennemgang af informationssikkerhed

18.2.1 Uafhængig gennemgang af informationssikkerhed

Overvågning og audit af outsourcing leverandør

Leverandøren skal levere rapportering for, i hvilken grad aftalte servicemål er opfyldt.

Kommunen kan foretage audit af leverandøren, alternativt kan intern auditrapport, it-revisionsrapport, årlig risikovurdering eller it-outsourcing-erklæring indgå i overvågningen.

18.2.2 Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder

Overholdelse af standarder

Sikkerhedssystemet overholder kravene i International Standard ISO/IEC 27002, på de områder, hvor kommunens risikovurdering retfærdiggør overensstemmelse og tilhørende sikkerhedsinvesteringer.
Sikkerhedssystemet overholder kravene i International Standard ISO/IEC 27001 på de områder, hvor kommunens risikovurdering retfærdiggør overensstemmelse og tilhørende sikkerhedsinvesteringer.

18.2.3 Undersøgelse af teknisk overensstemmelse

Sikkerhedstest af interne it-systemer

Mindst en gang om året skal der udføres uddybende sikkerhedstest af sikkerhedsniveauet i internt netværksudstyr og servere.

Sikkerhedstest af eksterne it-systemer

Mindst en gang om året skal der udføres sikkerhedstests af kontroller og netværksforbindelser for at identificere og undgå uautoriserede adgangsforsøg.

Omfang af informationssikkerhedspolitik

Informationssikkerhedspolitikken skal så vidt muligt være uafhængig af anvendt teknologi.

Revision af informationssikkerhedspolitikken

Der skal ske revision af sikkerhedspolitikken mindst en gang om året.
Sikkerhedspolitikken skal gennemgås, når der sker vigtige ændringer i it-miljøet.

Definitioner

Virksomheden anvender de definitioner, der er angivet i GDPR, når dette ikke udgør en konflikt med eksisterende terminologi.

.