Hjørring Kommune

Regler

Informationssikkerhedsregler for hvert kontrolmål i ISO 27002:2013. Gældende for embedsmænd og folkevalgte i Hjørring Kommune. Godkendt af I-sikkerhedsudvalget den 13-12-2017

2.0

15-12-2017

Indholdsfortegnelse

5 I-sikkerhedspolitikker

5.1 Regler for styring af I-sikkerhed

5.1.1 Politikker for I-sikkerhed

Omfang af I-sikkerhedspolitik
I-sikkerhedspolitikken er en integreret del af Hjørring Kommunes overordnede I-sikkerhedspolitik.
I-sikkerhed defineres som de samlede foranstaltninger til at sikre fortrolighed, tilgængelighed og integritet.
Foranstaltninger inkluderer tekniske, proceduremæssige, regel- og lovmæssige kontroller.

Publicering af I-sikkerhedspolitik
I-sikkerhedspolitikken offentliggøres og kommunikeres til alle relevante interessenter herunder alle medarbejdere.

5.1.2 Gennemgang af I-sikkerhedspolitikker

Vedligeholdelse af I-sikkerhedspolitik
I-sikkerhedspolitikken vedligeholdes af I-sikkerhedskoordinator. Ændringer i den overordnede I-sikkerhedspolitik skal godkendes af Byrådet. Ændringer i retningslinierne skal godkendes af I-sikkerhedsudvalget.
I-sikkerhedspolitikken med tilhørende retningslinier revideres 1 gang årligt.

6 Organisering af I-sikkerhed

6.1 Intern organisering

6.1.1 Roller og ansvarsområder for I-sikkerhed

Sikkerhedsorganisation
Direktionen har det overordnede ansvar for I-sikkerheden i Hjørring Kommune. Organisering af I-sikkerhedsområdet fremgår af den overordnede I-sikkerhedspolitik.

Hjørring Kommune har et forum for I-sikkerhed - kaldet I-sikkerhedsudvalget - der har ansvar for at sikre, at strategien for I-sikkerhed er synlig, koordineret og i overensstemmelse med kommunens mål.
Der findes en separat og veldefineret sikkerhedsfunktion, hvis primære arbejdsopgave er at sikre Hjørring Kommune. Denne kaldes I-sikkerhedsadministrationen.

Systemoversigt og systemejerskab
Der udpeges en systemejer for alle systemer i Hjørring Kommune. Systemejerskab placeres på kontorchefniveau. Systemejer har ansvar for anskaffelse, vedligeholdelse og drift. Ansvar for systemer, risikovurdering og beredskabsplanlægning kan ikke uddelegeres. Der henvises til bilag, som viser hvem der er systemejer (Kitos).
Sikkerhedsansvarlige systemejere for forretningskritiske systemer skal identificeres og gøres opmærksom på dette ansvar. Disse ejere skal have ansvar og beføjelser til at sikre tilstrækkelig beskyttelse.

Behandlingsfortegnelse
Kommunen skal føre en intern, skriftlig fortegnelse over behandlingsaktiviteter. Ansvaret for vedligeholdelsen af denne påhviler I-sikkerhedskoordinator.
Koordination af I-sikkerheden

Ansvaret for koordination af I-sikkerheden på tværs i organisationen varetages af I-sikkerhedsudvalget.
Koordinering af I-sikkerheden udføres og varetages i praksis af I-sikkerhedskoordinator.

IT-drift
IT-afdelingen er ansvarlig for, at egne sikkerhedsregler og procedurer i forhold til IT-driften følges, samt at problemer og fejl opdages, udbedres og rapporteres.
IT-afdelingen indgår i det løbende arbejde (forslag og implementering) med forbedrede sikkerhedstiltag (procedurer, metoder, services).

6.1.2 Funktionsadskillelse

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

Funktionsadskillelse: udvikling, test og driftsmiljøer
Adgang til og behandling af data må kun ske ud fra aktuelle behov og sådan, at der er klar adskillelse mellem udvikling, vedligeholdelse, test og drift.
Tilsvarende bør der være en klar adskillelse mellem de planlæggende, udførende og kontrollerende funktioner i det omfang, det er organisatorisk muligt.

6.1.3 Kontakt med myndigheder

Kontakt med relevante myndigheder
Kommunen skal være bekendt med de væsentligste kontakter hos offentlige myndigheder i relation til kommunens sikkerhed og virke. Der skal udarbejdes en oversigt over, hvem i kommunen der har kontakt med hvilken myndighed i en given situation.
Brand
Indbrud, hærværk
I-sikkerhedsbrud
Miljø
andet...
Der henvises i øvrigt til kommunens beredskabsplan

Ved brud på sikkerheden er der etableret en procedure for håndtering af bevismateriale og eventuelt kontakt med relevante myndigheder, se iøvrigt dette regelsæts kapitel 16.
Hvis tredjepart behandler personoplysninger, skal denne underrette den registeransvarlige hvis et brud på persondatasikkerheden er opstået. Der skal foreligge databehandleraftaler, hvoraf dette krav fremgår. se iøvrigt dette regelsæts kapitel 15.

6.1.4 Kontakt med særlige interessegrupper

Information om nye trusler, virus og sårbarheder
IT-afdelingen holder sig orienteret inden for de benyttede platforme.
IT-afdelingen informerer I-sikkerhedskoordinator om nye trusler, som potentielt kan berøre sikkerheden i Hjørring Kommune.
Der er udpeget en ansvarlig gruppe bestående af lT-driftschef, netværksmedarbejder og servermedarbejder, som sikrer en dialog omkring identifikation af nye sårbarheder.

Kontakt med interessegrupper og fora
Hjørring Kommune skal oparbejde og vedligeholde kontakt med sikkerhedsfaglige interessegrupper.

6.1.5 I-sikkerhed ved projektstyring

Projektmodellen skal indeholde følgende overvejelser omkring I-sikkerhed:

- Kravspecifikationen skal indeholde kravene til I-sikkerhed.
- Identifikation af nødvendige sikringstiltag skal blandt andet gøres ved hjælp af risikovurderinger.
- I-sikkerhed skal være en integreret del af projektledelse.
- Hjørring Kommunes Kravspec-generator kan anvendes som et interaktivt værktøj til brug ved etablering af kravspcifikationer til leverandører, men det er ikke et krav.

6.2 Mobilt udstyr og fjernarbejdspladser

6.2.1 Politik for mobilt udstyr

Der er udarbejdet procedure for anvendelse af mobilt udstyr. Proceduren findes i proceduresamlingen i SecureAware.

Sikkerhedskontroller for mobilt udstyr
Bærbare pc'ere med Windows og Mac OS, samt tablets med Windows OS sikres med antivirus og firewall. Adgangskontrolsystemer indføres på alle mobile enheder, herunder smartphones, bærbare og tablets/Ipads. Disse foranstaltninger opdateres løbende.

Brug af privat udstyr
Det er tilladt at koble privat udstyr op mod arbejdspladsens informationssystemer. Der er udarbejdet procedurer for brug af privat udstyr. Se proceduresamlingen i SecureAware.

6.2.2 Fjernarbejdspladser

Forsikringsdækning for mobile enheder
Fagområderne kan, hvis de ønsker det, sikre at der er etableret passende forsikringsdækning i forbindelse med opbevaring og anvendelse af IT-udstyr uden for kommunens netværk.

7 Personalesikkerhed

7.1 Før ansættelsen

7.1.1 Screening

Ved besættelse af stillinger, hvor dette er relevant, skal ansøgeren forud for ansættelse erklære at være ustraffet, samt ikke at være sigtet eller tiltalt i verserende sager. Der henvises i øvrigt til Hjørring Kommunes politik for indhentning af straffeattester, som fås ved henvendelse til Løn og Personale.
I situationer hvor det skønnes nødvendigt indhentes der personlig reference ved ansættelse af nye medarbejdere.
Leder med ansvar for ansættelsen skal tilse, at der sker forsvarligt baggrundscheck af IT-medarbejdere samt medarbejdere med ansvar for forretningskritiske arbejdsområder ved indhentning af straffeattest og referencer.

7.2 Under ansættelsen

7.2.1 Ledelsesansvar

Lederens I-sikkerhedsmæssige ansvar overfor medarbejderne findes beskrevet i introduktion til lederens i-sikkerhedsansvar i proceduresamlingen i SecureAware.

7.2.2 Medarbejderansvar

Det er den enkelte medarbejders personlige ansvar, at betjene det maskinel og programmel, der stilles til rådighed efter de retningslinier, regler og forskrifter, der gives fra systemansvarlige, leverandører og IT-afdelingen.
Kun IT-medarbejdere og leverandører må foretage indgreb i systemopsætninger og maskinel, herunder forsøg på at omgås sikkerhedsforskrifter og dette kun i testøjemed.

7.2.3 Bevidsthed om og uddannelse i I-sikkerhed

Undervisning i I-sikkerhedspolitikken
Alle medarbejdere skal have undervisning i kommunens I-sikkerhedspolitik og baggrundsviden omkring denne. Dette sker bl.a. ved løbende og tilbagevendende awarenesskampagner af forskellig art. Ansvaret for dette påhviler nærmeste leder.
Medarbejdernes kendskab, forståelse og efterlevelse af I-sikkerheden vurderes jævnligt ved hjælp af en brugerundersøgelse. Awareness aktiviteter tilrettes ud fra resultaterne af brugerundersøgelsen.

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

7.2.3.1 Opmærksomhed om I-sikkerhed generelt

Opmærksomheden rettes mod ændrede reaktionsmønstre i systemerne og mod ukendte personer. I IT-afdelingen skal ukendte personer kontaktes om deres ærinde. Afvigelser fra det normale rapporteres til nærmeste leder.
Af hensyn til sikkerheden overvåges og logges al aktivitet på kommunens netværk. Dette gælder både aktivitet i fagsystemer, på internettet, via email og lignende.
I henhold til Persondataloven foretages der halvårlig logkontrol i Borgerservice.

7.2.4 Sanktioner

Overtrædelse af sikkerhedsretningslinierne
Det er ledelsens ansvar, at sanktioner for brud på kommunens politikker, regler eller retningslinier håndhæves konsekvent og i overensstemmelse med gældende lovgivning.
Det er ikke tilladt at foretage uautoriseret afprøvning af sikkerheden.
Det er ikke tilladt at forsøge at omgå sikkerhedsmekanismer.
Hændelser hvor medarbejdere er involverede, bliver håndteret konsekvent i overensstemmelse med gældende personalepolitik.
Bevidste eller gentagne overtrædelser vil medføre disciplinære sanktioner.

7.3 Ansættelsesforholdets ophør eller ændring

Ansættelsesforholdets ophør eller ændring

Ved ansættelsesforholdets ophør eller ændring er det nærmeste leders ansvar at proceduren for denne situation overholdes. Se proceduren for fratrædelse i SecureAware.

Ansættelsesforholdets ændring

Ved ændring af en medarbejders arbejdsopgaver skal nærmeste leder gennemgå medarbejderens adgange og rettigheder.

8 Styring af aktiver

8.1 Ansvar for aktiver

8.1.1 Fortegnelse over aktiver

Registrering af IT-udstyr

Alle fysiske aktiver (arbejdsstationer, bærbare computere, tablets/Ipads og mobiltelefoner) registreres i registreringssystem af IT-afdelingen med angivelse af serienumre, ejerskab og evt. ibrugtagningsdato, udlånsregistrering, serviceaftaler, forsikring mv.

8.1.2 Ejerskab af aktiver

Sikkerhedsansvar for informationsaktiver

Inventarlister over informationsaktiver og IT-udstyr med tilhørende ansvarlige ejere udarbejdes og vedligeholdes. Ejere betyder de personer der er ansvarlige for sikker drift af udstyret.
Afdelingen for Innovation og Digitalisering har - i samarbejde med superbrugere i fagområderne - ansvaret for vedligeholdelse af en liste over samtlige informationssystemer. Det er systemejerens ansvar at sikre, at data er opdateret også i forbindelse med ændringer i ejerskabet.

8.1.3 Accepteret brug af aktiver

Kryptering af privat udstyr

Der er ikke særlige krav til kryptering af privat udstyr.

Brug af cloud løsninger

Kun Cloud-løsninger som IT-afdelingen har godkendt til brug, må anvendes. IT-afdelingen vurderer om der er sikkerhedsmæssige risici forbundet med anvendelsen af cloudløsninger.
Cloud-løsninger må anvendes, hvis der er et forretningsmæssigt behov og der ikke er væsentlige sikkerhedsmæssige risici forbundet med løsningen.

Brug af sociale netværk

Ansattes brug af sociale netværk må ikke genere almindelig drift og brug af kommunens IT-systemer. Omfanget af anvendelse af sociale netværk i arbejdstiden aftales i samarbejde med nærmeste leder.
Persondata aldrig må deles på sociale netværk.
Se retningslinierne for brug af de sociale medier i SecureAware under ”Vejledning for brug af sociale medier i arbejdstiden”.

Privat anvendelse af kommunens internetforbindelse
Al trafik på Hjørring Kommunens internetforbindelse der ikke er arbejdsrelateret og som ikke foretages for at løse en konkret arbejdsopgave anses for at være privat.
Download og programmering af programmel, musik, spil mv.
Som udgangspunkt er kommunens pc'ere installeret med det programmel, der er nødvendigt for at løse den enkeltes arbejdsopgaver. I takt med, at behovet øges eller mindskes sørger IT-afdelingen for at installere eller afinstallere programmel eller regulere i de tildelte rettigheder, efter anmodning fra nærmeste leder.
Det er ikke tilladt at installere programmel, der krænker 3. parts rettigheder. Det er tilladt at installere meget udbredt og anerkendt programmel. Her tænkes på programmel til netbank, musikafspilning, filorganisering og -søgning, billedredigering og digitale signaturer. Er man i tvivl kontaktes IT-afdelingen, som vurderer de sikkerhedsmæssige aspekter.
Al software installeres fra IT-afdelingen igennem system til udrulning af software.

Privat brug af email
Oplysninger på kommunens netværk er som udgangspunkt betragtet som kommunens ejendom. Dette gælder også private emails sendt til og fra kommunens netværk.
Det accepteres at benytte email til private beskeder i rimeligt og begrænset omgang. Private emails skal mærkes PRIVAT og eventuelt gemmes i en mappe mærket PRIVAT.
Private emails er ikke undtaget fra at kunne åbnes i helt særlige tilfælde som langvarig sygdom, dødsfald eller mistanke om misbrug af beføjelser. Åbning af medarbejdernes emails i ovennævnte tilfælde sker kun efter forudgående underretning af medarbejderen (der skal dog ikke gives samtykke fra medarbejderen) og kun på anmodning fra områdedirektøren eller nærmeste leder alt efter karakteren af behovet for åbning.

8.1.4 Tilbagelevering af aktiver

Ved en medarbejders fratrædelse skal udleveret aktiver sikres samt data på disse og privat udstyr skal slettes. For at sikre processen skal ”Proceduren for fratrædelse og ændring af arbejdsopgaver” følges. Nærmeste leder er ansvarlig for at dette sker.

8.2 Klassifikation af information

8.2.1 Klassifikation af information

Data klassificeres efter den til enhver tid gældende klassifikationsmodel, som findes i SecureAware.
Informationer og data skal klassificeres som følger:
Offentlig information: Alt materiale der må udleveres til offentligheden, inkl. Information tilgængelig på hjemmeside, generel information til kunder, offentlige nyhedsbreve etc.
Intern information: Informationer på intranet, interne emails, procedure, retningslinier for kommunen, telefonlister etc. Disse informationer er forbeholdt kommunens medarbejder til internt brug.
Fortrolig information: Disse informationer tæller informationer der er vigtige for kerneområdet i forretningen, regnskaber, kontrakter, risikovurderinger etc.
Personfølsom information: Data der er relateret til et individ, f.eks. en kunde, en borger, en patient eller en medarbejder. Her kan bl.a. være tale om helbreds- og medicinske oplysninger, religiøse og politiske tilhørsforhold.
Uddannelse i klassificering af informationer
Alle ansatte skal modtage instruktioner om, hvordan data og dokumenter klassificeres. Ansvaret for dette påhviler nærmeste leder.

Ansvar for klassifikation
Aktivets ejer har ansvaret for, at aktivet er klassificeret.

8.2.2 Mærkning af information

Forretningsgangen for beskyttelse af datamediers indhold skal omfatte:
- Klar mærkning af alle kopier.
- Adgangsbegrænsning.
- Fysiske krav til opbevaringssted, f.eks. temperatur og luftfugtighed ifølge leverandørens specifikationer.
- Minimering af distribution.

8.2.3 Håndtering af aktiver

Tyveri eller bortkomst af mobilt udstyr
Medarbejderen er ansvarlig for at privat udstyr, der anvendes til behandling af kommunens informationer, opbevares på forsvarlig vis.
IT-afdelingen skal kontaktes straks, i tilfælde af tyveri/bortkomst af enheden.
IT-afdelingen kan slette indeholdet på mobilt udstyr, hvis man har synkroniseret det med sin webmail. Alt indehold på det mobile udstyr slettes, hvilket også er gældende ved brug af privat udstyr. Der henvises i øvrigt til procedure for brug af eget udstyr. Proceduren findes på medarbejderweb og i SecureAware.

8.3 Mediehåndtering

8.3.1 Styring af bærbare medier

Brug af bærbare medier til fortrolige data
Fortrolige informationer må ikke opbevares eller gemmes på bærbare medier, f.eks. USB-hukommelse, tablets, telefoner eller dvd'er.

8.3.2 Bortskaffelse af medier

Bortskaffelse og genbrug af medier
Beholdere med papirmateriale til destruktion skal holdes aflåste.
Alle datamedier skal slettes inden genbrug.
Hvis en ekstern leverandør benyttes til destruktion af kommunens datamedier, skal det sikres at leverandøren efterlever de aftalte sikkerhedskrav.
Alle datamedier f.eks. harddiske, disketter, cd'er, dvd'er, bånd og hukommelsesenheder skal destrueres eller afleveres til IT-afdelingen, som sørger for sletning og evt. destruktion.

8.3.3 Fysiske medier under transport

Brug af datamedier
Udstyr eller medier, der indeholder fortrolig information må kun forsendes med sikker kurer, eller via en præcis sporbar leveringsmetode.
Benyttelse af bærbare datamedier skal være forretningsmæssigt begrundet.

9 Adgangsstyring

9.1 Forretningsmæssige krav til adgangsstyring

9.1.1 Politik for adgangsstyring

Brugeradministration, outsourcingleverandør
Leverandøren skal følge kommunens regler for brugerstyring.

Begrænset adgang til informationer
Adgang til systemfunktioner og informationer for brugere og personer med supportfunktioner skal administreres efter princippet: blokering af adgang til alt andet end det, som specifikt er tilladt.
Brugere og medarbejdere med supportfunktioner må kun få adgang til systemfunktioner og informationer, hvis dette er forretningsmæssigt begrundet.

Inddragelse af privilegier ved fratrædelse
Ved en medarbejders fratrædelse er det nærmeste leders ansvar at sørge for, at samtlige privilegier inddrages. Nærmeste leder skal til denne proces følge ”Proceduren for fratrædelse og ændring af arbejdsopgaver”, som findes i SecureAware.

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 konfigureres som standard til at blokere al anden adgang end den, som er specifikt tilladt.
Der er implementeret et automatiseret adgangskontrolsystem, som dækker samtlige systemkomponenter.
IT-afdelingen sikrer ved styring af brugernes netværksadgang imod uautoriseret anvendelse af fælles netværk og hertil knyttede tjenester.

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

Adgang til trådløse netværk
Brugere autentificeres ved hjælp af et bruger-ID og adgangskode, før der gives adgang til kommunens trådløse netværk. Der er undtagelser for bibliotekerne og Borgerservice.

Overvågning af netværk
IT-afdelingen skal have den nødvendige viden og redskaber til overvågning af kommunens netværk, f.eks. til fejlretning samt detektering og sporing af sikkerhedshændelser.
IT-afdelingen er ansvarlig for kontinuerligt at overvåge brugen og sikkerheden af kommunens netværksinfrastruktur. Driftsafdelingen er ansvarlig for identificering, diagnosticering, løsning og rapportering af hændelser, samt for samarbejde med andre interessenter.
IT-afdelingen overvåger løbende netværk med henblik på detektering af brud på sikkerheden.
IT-afdelingen udfører årligt evalueringer af regler for netværkstrafik i firewalls og routere.

Autentificering ved adgang til netværket
Fjernadgang til det interne netværk beskyttes ved hjælp af VPN eller via Citrix.

To-faktor autentifikation benyttes ved fjernadgang til det interne netværk.

Retningslinier for brug af netværkstjenester
Det er IT-afdelingens ansvar at sørge for, at brugere kun har adgang til de tjenester, de er autoriseret til at benytte.

9.2 Administration af brugeradgang

9.2.1 Brugerregistrering og -afmelding

Identifikation og autentifikation af brugere
Der benyttes en passende autentifikationsteknik til verifikation af brugernes identitet.
Alle brugere har en unik identitet til personlig brug.
Brugeridentiteten kan spores til den person, som er ansvarlig for en given aktivitet.
Der må ikke anvendes fælles adgangskoder eller brugerprofiler. Undtaget er bibliotekerne og Tandplejen.

Brugeradministration, cloudløsning
Hjørring Kommune skal sikre, at der er etableret procedurer, der sikrer en tilstrækkelig brugerstyring, herunder at der sker nedlukning ved afsked og at der er nødprocedurer for lukning af medarbejdere, som forlader arbejdspladsen pludseligt eller uventet.
Kommunen skal sikre at der er sporbarhed, således at det er muligt at kunne logge brugeres adgang til klassificerede informationer.

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

Gennemgang af brugerprofiler
Alle brugerprofiler gennemgås mindst en gang årligt for at identificere inaktive profiler eller tilsvarende, der skal fjernes eller ændres. Dette gøres af nærmeste leder i samarbejde med IT-afdelingen.

9.2.2 Tildeling af brugeradgang

Registrering af brugere
Serviceleverandørerer skal anvende tilsvarende eller samme autorisationsprocedure som kommunen.
Brugere modtager en skriftlig bekræftelse af de tildelte rettigheder.

Tildeling af adgang og rettigheder til kommunens systemer og data foregår efter funktions- og opgavebehov.
IT-medarbejdere tildeles særskilt bruger-ID til brug for arbejde med tekniske opgaver. Administration af brugerne i systemerne skal udføres under hensyntagen til funktionsadskillelse.
Brugeradministration skal underbygges af skriftlig dokumentation (email sendes til IT-servicedesk) fra nærmeste leder til brug for kontrol og revision.
Ændring af brugeradgang og rettigheder til systemer og data ændres umiddelbart i forbindelse med, at en medarbejder skifter funktion eller afdeling. Ændringerne rekvireres skriftligt af nærmeste leder. Kontrol af adgang og rettigheder undergår en periodisk stikprøvevis revision. Stikprøvekontrol foretages af nærmeste leder.

IT-afdelingen vedligeholder fortegnelser over, hvordan bruger-ID eller rettigheder fjernes eller ændres ved

ophør eller ændring af brugeres jobfunktion.

9.2.3 Styring af priviligerede adgangsrettigheder

Skift af administratoradgangskode ved fratrædelse
Når en person med kendskab til administrative adgangskoder fratræder, lukkes dennes adgang til systemerne.

Tildeling af brugerrettigheder
Nærmeste leder anmoder IT-afdelingen om at tildele relevante brugerrettigheder til kommunens IT-systemer.

Administration af privilegier
Administratorkonti må ikke benyttes til ikke-administrative opgaver.
Konti med administrative rettigheder skal tildeles til særskilte og personlige bruger-ID.

Udvidede adgangsrettigheder
Der benyttes særlige brugeridentiteter til de udvidede rettigheder af hensyn til overvågning og opfølgning.
De udvidede adgangsrettigheder er registreret i AD.
De udvidede adgangsrettigheder må kun tildeles i begrænset omfang og alene ud fra et arbejdsbetinget behov.

Ændring af administrative adgangskoder
Administrative adgangskoder ændres hvis udenforstående får kendskab til disse.
Administrative adgangskoder følger samme minimumsregler som øvrige adgangskoder.
Administrative adgangskoder ændres hvert kvartal.

9.2.4 Styring af hemmelig autentifikationsinformation om brugere

Overdragelse af adgangskode
Adgangskoder må ikke overdrages på ukrypterede forbindelser, f.eks email. men kan i særlige tilfælde overdrages verbalt, f.eks. over telefon.
I forbindelse med dataudveksling skal adgangskoder altid sendes krypteret.

Retningslinier for adgangskoder
Til dette følges proceduren om adgangskoder, som findes i SecureAware.

9.2.5 Gennemgang af brugeradgangsrettigheder

Gennemgang af brugerautorisationer
Systemejer er ansvarlig for halvårligt at kontrollere samtlige brugerautorisationer.
Gennemgang af administrator adgang
Brugere med administrator adgang skal gennemgås hver 3. måned (oftere end normale brugere). Systemejere har ansvaret for dette.

9.2.6 Inddragelse eller justering af adgangsrettigheder

Brugerprofiler for konsulenter og deltidsansatte
Midlertidigt personale tildeles ikke normalt adgang til alle IT-systemer. Adgang kan tildeles efter godkendelse fra systemejer eller nærmeste leder.
Eksterne samarbejdspartnere med behov for adgang til et IT-system i forbindelse drifts-, udviklings- og vedligeholdelsesopgaver, skal autoriseres hertil. Såfremt systemet indeholder personoplysninger skal der indgås en databehandleraftale. Der skal under alle omstændigheder som minimum underskrives en

tavshedserklæring.
Autorisation af eksterne samarbejdspartnere må kun finde sted, såfremt en entydig identifikation af den pågældende medarbejder kan finde sted. Dette skal som udgangspunkt ske i form af navn, cpr.nr, telefonnummer og emailadresse.
Autorisationen sker på baggrund af en anmodning fra den ansvarlige for aftaleindgåelsen med den eksterne samarbejdspartner.
Ved udveksling af personoplysninger, fortrolige oplysninger og kritiske data i form af udtræk fra fra et system til et andet (dataudveksling skal de nærmere omstændigheder for udvekslingen afklares. Ansvaret for denne afklaring påhviler den, som foranlediger udtrækket foretaget.

9.3 Brugernes ansvar

9.3.1 Krav til sikre adgangskoder

Retningslinier for adgangskoder
Personlige adgangskoder skal skiftes periodisk, hvilket sker systemstyret. Adgangskoder må kun noteres på en sikker måde og må aldrig videregives til andre. Personlige adgangskoder til IT-systemerne skal være tilstrækkelige komplekse indenfor de rammer, som de enkelte IT-systemer stiller til rådighed og følge kommunens regler for adgangskodeopbygning. Systemerne skal så vidt muligt kontrollere opbygningen automatisk. I proceduren for adgangskoder findes krav til opbygningen samt regler forbundet med adgangskoder. Denne procedure findes i SecureAware.

9.4 Styring af system- og applikationsadgang

9.4.1 Begrænset adgang til informationer

Fjernadgang 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 funktionalitet og data i informationssystemer
Informationssystemer skal overholde kommunens procedure for adgangskontrol.
Procedurerne er baseret på en risikovurdering og på de forretningsmæssige behov.

9.4.2 Procedurer for sikker log-on

Automatiske afbrydelser
Funktioner i et fagsystem, der ikke har været aktivt i et fastlagt tidsrum, bliver automatisk afbrudt.

Sikre login-procedurer skal indbefatte følgende:
- At data fra systemet eller applikationen ikke vises ved login.
- Vise en advarsel om, at kun autoriserede brugere kan få adgang til systemet.
- Begrænsning af oplysninger, der kan benyttes af en uautoriseret bruger i forbindelse med login.
- Beskyttelse mod hacker login-forsøg.
- Logning af succesfulde login-forsøg.
- Logning af mislykkede login-forsøg.
- At indtastede adgangskoder ikke vises.
- At der ikke sendes adgangskoder i klartekst over netværk.

Sikker log-on

Systemadgang beskyttes af en sikker log-on-procedure.

9.4.3 Brug af priviligerede systemprogrammer

Brug af systemværktøjer
Hvor funktionsadskillelse er påkrævet, må brugere ikke have adgang til både systemværktøjer og brugersystemer.
IT-afdelingen skal begrænse og styre adgangen til systemværktøjer, f.eks. utilities, der kan påvirke eller omgå systemers eller enheders sikkerhed.

10 Kryptografi

10.1 Kryptografiske kontroller

10.1.1 Politik for anvendelse af kryptografi

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

10.1.2 Administration af nøgler

Nøglehåndtering
Procedurer for nøglehåndtering skal beskrive, hvordan uautoriseret udskiftning af nøgler forhindres samt, hvordan opdeling af samlet kendskab til nøgler på to eller tre personer foregår.
IT-afdelingen skal etablere et nøglehåndteringssystem, som understøtter kommunens anvendelse af kryptografi.
Proceduren for nøglehåndtering skal beskrive hvordan generering, distribution, opbevaring og destruktion af nøgler håndteres.
Proceduren for nøglehåndtering skal beskrive hvordan tilbagekaldelse af gamle eller ugyldige nøgler håndteres.

11 Fysisk sikring og miljøsikring

11.1 Sikre områder

11.1.1 Fysisk perimetersikring

Kommunens ydre områder er anlagt på en måde, der sikrer mod uretmæssig adgang og som samtidig styrer gæsters adgang til og færden omkring kommunens følsomme data og tekniske installationer. Dette sker i praksis ved, at bygningerne ved hjælp af det elektroniske låsesystem er delt op i borgerzoner og arbejdszoner. Der kan være andre eller yderligere specifikationer for kommunens decentrale institutioner.

Sikre områder er defineret som IT-afdelingen og serverrum.

Aflåsning af lokaler og bygninger
Alle døre og vinduer skal kunne låses forsvarligt.
Overvågning i sikre områder
Videokameraer som benyttes til overvågning af sikre områder, er placeret inden for det sikre område eller på anden vis beskyttet mod modifikationer og deaktivering.

IT-afdelingen sørger for, at arbejde i sikre områder overvåges.
Videooptagelser fra sikre områder opbevares i mindst en måned.

Videoovervågning generelt

Offentlige områder, der videoovervåges skal mærkes tydeligt. Forinden en ny videoovervågning etableres skal der foretages en analyse af behandlingsaktivitetens konsekvenser for de registreredes rettigheder og frihedsrettigheder. Ansvaret for konsekvensanalysen er den dataansvarliges. Den dataansvarlige skal inddrage kommunens DPO i udarbejdelsen af konsekvensanalyse.

Adgang til IT-kontorer og IT-teknikrum

Kommunens IT-medarbejdere har adgang efter behov. Adgangskontrol er i relevant omfang sikret med elektronisk låsesystem, som kan styre og registrere adgangen. De tildelte adgange undergår revision mindst én gang årligt af IT-ledelsen.
Rengøringspersonale må ikke gøre rent i server- og teknikrum.
Leverandører af IT-materiel eller anden teknik må kun have adgang til kommunens IT- og teknikrum efter aftale.
Faste systemkonsulenter må gives adgang til kommunens lokaler, maskiner og systemer i relation til formålet, på linie med kommunens medarbejdere.
Ingen tilkaldte (ukendte) teknikere må få adgang til kommunens IT- og teknikrum uden at oplyse firmanavn, navn og arbejdsperiode.
Eksterne systemudviklere med behov for adgang til kommunens IT-systemer og data, clearea og godkendes af kommunen. Adgang og rettigheder tildeles i forhold til det, der er nødvendigt for at løse opgaven.
De medarbejdere eller afdelinger der har periodiske gæster er ansvarlige for deres færden.
Vikarer og afløsere i IT-afdelingen må kun have adgang til kommunens serverrum, teknikrum eller tilsvarende i følge med anden medarbejder.

Gæsters adgang

Gæster må aldrig bevæge sig uledsaget rundt på arbejdspladsen. Den ansvarlige medarbejder sørger for at ledsage gæster til den aftalte lokation.
Faste samarbejdspartnere kan, efter aftale med den ansvarlige medarbejder, selv bevæge sig til den aftalte lokation.

Indbrudsalarmer

Hjørring Kommune anvender passende alarmsystemer på samtlige bygninger og lokaler.

Adgang til og sikring af IT-kontorer

Kontorer som benyttes af IT-medarbejdere og hvor der forefindes reservedele, softwarepakker mv. er sikre mod uvedkommendes fri adgang og mod tyveri.
Afdelingens adgangsdøre er aflåst, når lokalerne er ubemandede. Effekter af speciel interesse for tyve opbevares i aflåste enheder, når det ikke anvendes.
Generelt udvises der omhyggelighed med hensyn til oprydning.

11.1.2 Fysisk adgangskontrol

Adgangskort

Adgang til Hjørring Kommunes administrative bygninger reguleres med adgangskort, som udleveres på første arbejdsdag af nærmeste leder.

Adgangskort til håndværkere og andet midlertidigt personale

Serviceafdelingen har ansvaret for, at håndværkere og andet midlertidigt personale kun færdes de steder, hvor de har ærinder. Adgangen reguleres med adgangskort.
IT-afdelingen har adgangskort med særlige adgange, der giver adgang til IT relevante områder. Hvis disse skal bruges, skal proceduren for udlån af adgangskort følges. Denne findes i IT-afdelingen.

11.1.3 Sikring af kontorer, lokaler og faciliteter

Placering af IT- og teknikrum i bygningen
Centralt og fælles IT-udstyr, samt andet sårbart teknisk udstyr er placeret i aflåste lokaler beregnet alene til formålet. Lokalerne er ikke markeret med skiltning.

Placering af IT-udstyr i teknikrum
IT-udstyret er placeret i reoler og racks med plads til betjening og servicering fra begge sider.

Sikring mod fugt og vandskader - alarmering
Udstyr må ikke placeres nær eller under gennemgående vandrør. Der tages særlige hensyn omkring ovenlysvinduer mod utætheder og indtrængende vand.

Adgang og sikring af mødelokaler
Kommunens møde- og undervisningslokaler kan frit benyttes af kommunens medarbejdere til arbejdsrelaterede formål. Mødeværten er ansvarlig for eksterne deltageres færden i området.

11.1.4 Beskyttelse mod eksterne og miljømæssige trusler

Opbygning, placering og indretning af IT-rum skal ske under hensyntagen til eksterne forhold, som kan true stabiliteten, såsom strømafbrydelser, elektrisk støj og rystelser fra andet maskinel i bygningen, ligesom den løbende forsyning af strøm og ventilation skal være tilgodeset. For at begrænse behovet for adgang til disse områder, skal IT-rum og teknisk forsyning være adskilt fra andre rum og funktioner.

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

Forsyningssikkerhed
I forhold til serverrum har IT-afdelingen ansvaret for, at alle forsyninger som elektricitet, vand, kloak, varme og ventilation har den fornødne kapacitet og løbende inspiceres for at forebygge uheld, der kan have indflydelse på informationsaktiverne.
Data- og telekommunikationsforbindelser er etableret via minimum to adgangsveje for forretningskritiske systemer.

Brandsikring
Serverum er forsynet med lovmæssigt brandslukningsudstyr, samt med sensorer (røg, varme eller ion detektorer) til automatisk branddetektering, alarmering (evt. et Early Warning System) og med automatisk udløsning af slukningsmiddel.
Der må ikke opbevares brandbare materialer i rummene ligeom brug af åben ild ikke er tilladt.

11.1.5 Arbejde i sikre områder

På rådhuset er sikre områder defineret som IT-afdelingen og serverrum.

11.1.6 Områder til af- og pålæsning

Af- og pålæsningsområder
Af- og pålæsningsområder er indrettet, så risiko for uautoriseret adgang til kommunens 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 IT-afdelingen.

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

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

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

11.2.2 Understøttende forsyninger (forsyningssikkerhed)

Køling
IT- og teknikrum skal være sikret med tilstrækkelig og konstant ventilation og køling, der lever op til IT-leverandørernes specifikationer.
Der findes sensorer, som kan alarmere IT-medarbejderne eller andre ved væsentlig reduktion eller svigt i køling eller ventilation.

Nødstrømsanlæg
IT-udstyret skal fordeles på separate sikringsgrupper med spændingsudjævnere. Kritiske servere skal sikres mod strømudfald med UPS-udstyr. UPS'ens kapacitet afgøres ud fra konsekvensen af et nedbrud. IT-driften har ansvaret for at UPS'en afprøves én gang årligt.
Strømforsyningen skal være overvåget med alarm til IT-afdelingen eller andet.

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.
Kabler skal være sikret mod udrivning og brud. Krydsfelter skal være i aflåste skabe, hvortil adgangen begrænses. Alle kabelgennemføringer i murværk i forbindelse med serverrum skal være tilstoppet med brandhæmmende materialer.

11.2.4 Vedligeholdelse af udstyr

Vedligeholdelse af udstyr og anlæg
IT-afdelingen er ansvarlig for, at der føres log over alle fejl og mangler samt reparationer og forebyggende vedligeholdelse.
Kun godkendte leverandører må udføre reparationer og vedligeholdelse.

11.2.5 Sikring af udstyr og aktiver uden for organisationen

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

11.2.6 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 er IT-supports ansvar.

11.2.7 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.

11.2.8 Politik for ryddeligt skrivebord og blank skærm

Brug af adgangskodebeskyttet pauseskærm
Adgangskodebeskyttet skærmlås skal aktiveres på pc-arbejdspladser efter 15 minutters inaktivitet.

Opbevaring af fysiske dokumenter
Skriveborde skal ryddes for fortrolige dokumenter senest ved arbejdsdagens afslutning.
Dokumenter med personhenførbare oplysninger må ikke ligge med forsiden opad, når skrivebordet forlades.
Dokumenter med personhenførbare oplysninger skal opbevares i aflåst skab eller skuffe efter arbejdstid.
Fortrolige dokumenter skal opbevares i aflåst skab eller skuffe.

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

Driftsansvar

IT-afdelingen er ansvarlig for drift og administration af fælles IT-systemer, som f.eks emailsystem, samt disses sikkerhed. Dette inkluderer efterlevelse af I-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
Driftsafviklingsprocedurer for forretningskritiske systemer skal være dokumenterede, ajourførte og tilgængelige 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
Alle servere skal hærdes 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
Driftsafdelingen er ansvarlig for at identificere, logge og håndtere hændelser og afvigelser i driften af de IT-systemer de er ansvarlige for.
IT-afdelingen skal registrere væsentlige forstyrrelser og uregelmæssigheder i driften af systemerne samt årsager hertil. Alle iagttagelser skal registreres løbende og kunne samles til en periodisk rapportering.
Problemer og fejl af sikkerhedsmæssig karakter skal meddeles I-sikkerhedskoordinatoren.

12.1.2 Ændringsstyring

Planlægning, test og godkendelse af ændringer (Procedure beskrives IT)
Ændringer skal igennem en formaliseret godkendelsesprocedure inden drift.
Ændringer skal planlægges og afprøves inden de sættes i drift.
Ændringernes konsekvenser skal vurderes inden drift.

Ændringsstyring
- Der skal vedligeholdes en versionsstyring for alle systemændringer.
- Der skal indhentes godkendelse af ændringen fra systemejeren, før arbejdet med den går i gang.
- Der skal vedligeholdes et kontrolspor for alle ændringer.
- Driftsdokumentation og forretningsgange for brugerne skal holdes opdateret, således at de stadig er gældende efter ændringen.
- Ved ændringer skal der foregå en gennemgang af sikringsforanstaltninger og integritetskontroller for at sikre, at disse ikke forringes ved implementeringen.
- Der skal foretages test af driftsfunktionaliteten før ændringer gennemføres.

- IT-afdelingen skal oprette og vedligeholde procedurer for ændringsstyring for alle software- og systemkonfigurationsændringer (inklusiv netværksudstyr).
- Der skal foretages test af ændringer i netværk, firewall og routere.

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 forretningskritiske systemer.
Driftsafdelingen skal have procedurer, der minimerer risikoen for driftsstop som følge af manglende kapacitet.

12.1.4 Adskillelse af udviklings test- og driftsmiljøer

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

12.2 Beskyttelse mod malware

12.2.1 Beskyttelse mod malware

Beskyttelse mod skadevoldende programmer
Kommunens IT-systemer skal sikres mod infiltrering fra skadevoldende programmer gennem opsætning af relevante hardware- og softwarefiltre på servere, gateways, firewalls, arbejdsstationer, emailsystemer m.fl. Opsætningen skal være dokumeteret og følges ved fremtidige systemændringer og installationer.

Sikring mod adware og spyware
IT-enheder med direkte adgang til internettet skal sikres mod indtrængende spyware. Anti-spyware systemet skal jævnligt opdateres. Der skal periodisk køres total spyware kontrol på kritiske IT-enheder. Spor fra adware skal fjernes i samme eller tilsvarende kørsel. Bærbare computere skal opdateres ved tilslutning til kommunens netværk.

Sikring mod spam
Kommunen skal sikre sit emailsystem mod indgående spam gennem opsætning af filtre. Udgående emails filtreres for virus tilsvarende de indgående emails.
Medarbejderne skal være opmærksomme på, hvor mange modtagere, der indgår i en intern gruppeemail og begrænse udsendelse af ikke-arbejdsrelevante meddelelser og materialer i kommunens netværk.

Antivirus-programmer
Relevante IT-enheder med direkte eller indirekte adgang til internettet samt bærbare pc'ere skal være sikret med anti-virus software, som skal holdes opdateret. Bærbare PC'ere skal opdateres ved tilslutning til kommunens netværk.
Alle løse databærende medier skal viruskontrolleres automatisk inden brud. Der skal foreligge procedure til oprydning efter gennemført virusangreb. Alle indgående emails skal automatisk kontrolleres for vira.
Alle pc'er kontrolleres (scannes) automatisk for vira med faste intervaller.

Antivirus-produkter på systemer
IT-afdelingen skal sikre, at der er installeret aktive antivirus-produkter på samtlige computere i kommunen, og at disse opdateres højst et døgn efter leverandørens opdateringer.

Der skal etableres foranstaltninger til at sikre mod vira, orme, trojanske heste mv. Medarbejderne skal sikres den fornødne viden om disse gennem awareness kampagner.
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 indeholde filer modtaget over netværk eller via en hvilken som helst form for lagringsmedie, vedhæftede filer i emails og downloads, servere samt relevante endpoints såsom bærbare computere og arbejdsstationer.

Beskyttelse mod uønsket software
Godkendt antivirus-software skal anvendes, hvor dette er muligt.

Kontrol af antivirus på arbejdsstationer
Medarbejdere kan antage, at antivirus fungerer. Det er alene IT-afdelingens ansvar at kontrollere korrekt funktion.

12.3 Backup

12.3.1 Backup af information

Sikring af system- og konfigurationsfiler
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.
Datamedier til retablering af forretningskritiske systemer skal opbevares på et, for kommunen, eksternt opbevaringssted.

Sikkerhedskopiering og opbevaring af datakopier
Kommunens og systemteknisk data skal sikkerhedskopieres med faste intervaller og inden større systemomlægninger, eller inden at andre risikable aktiviteter påbegyndes.
Data og datakopierne skal opbevares adskilt fra de originale data og opbevares i et klassificeret databrandskab.
Data og datakopierne skal som minimum være placeret i god fysisk afstand fra originaldata, evt. i en anden bygning. Alternativt kan man benytte en fjernbackup service.

Backup af systemer og data
- IT-afdelingen er ansvarlig for sikker lagring og backup af data på serverudstyr.
- Backup skal være nøjagtig, fuldstændig og omfatte dokumenterede restore-procedurer.
- Backup-data skal beskyttes med passende logisk og fysisk adgangskontrol.
- Backup-data skal opbevares off-site, for at sikre redundans i tilfælde af katastrofer.
- Der skal jævnligt foretages afprøvning af restore-procedurer for at sikre validiteten af disse

Sikkerhedskopiering af data på andre systemer

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.

12.4 Logning og overvågning

12.4.1 Hændelseslogning

Opfølgningslogning
IT-afdelingen skal logge sikkerhedshændelser på kommunens væsentlige systemer.
IT-afdelingen skal sikre, at der foretages logning af al adgang til systemkomponenter (inklusive netværksudstyr).
IT-afdelingen skal logge fejlhændelser på kommunens væsentlige systemer.
IT-afdelingen skal logge væsentlige brugeraktiviteter på kommunens systemer.
IT-afdelingen skal logge fejlhændelser på kommunens systemer.
IT-afdelingen skal logge sikkerhedshændelser på kommunens systemer.

Opbevaring af opfølgningslog (OBS! Skal måske revurderes)
IT-afdelingen skal opbevare log for fejlhændelser på ethvert system i mindst 6 måneder.
IT-afdelingen skal opbevare log for sikkerhedshændelser på ethvert system i mindst 6 måneder.
IT-afdelingen skal opbevare log for brugerhændelser på ethvert system i mindst 6 måneder.

Hændelseslogning (OBS! skal måske revurderes)
Logning i forbindelse med alle systemkomponenter skal indeholde registrering af adgang til alle logs.
Loggen for systemkomponenter skal indeholde oprettelse og sletning af objekter på systemniveau.
Alle produktionssystemer skal logge information om adgang og forsøg på adgang, for at kunne spore uautoriseret aktivitet.
Alle sikkerhedshændelser skal logges og opbevares i en fastlagt periode af hensyn til opfølgning på adgangskontroller og eventuel efterforskning af fejl og misbrug.
Loggen for systemkomponenter skal indeholde al brug af identifikations- og autentifikationsmekanismer.

12.4.2 Beskyttelse af logoplysninger

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

12.4.3 Administrator- og operatørlog

Log-gennemgang
IT-afdelingen skal vedligeholde procedurer vedrørende daglig gennemgang af sikkerhedslogs og krav i forbindelse med opfølgning på uregelmæssigheder.
Logregisteringer fra servere, som udfører sikkerhedsfunktioner, eksempelvis Intrusion Detection Systems (IDS), autentifikation, autorisation og RADIUS, skal gennemgås dagligt.

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

12.4.4 Tidssynkronisering

Tidssynkronisering
Der skal benyttes NTP eller en lignende teknologi til tidssynkronisering.

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 jævnfør I-sikkerhedspolitikken. Brugerne må ikke ændre denne opsætning.

Installation af programmer på arbejdsstationer
Operativsystemer og applikationer må kun installeres og ændres af IT-afdelingen på godkendt udstyr.

Softwareopdateringer generelt
IT-afdelingen skal holde sig informeret om alle programrettelser til alle programmer, der anvendes i kommunen og snarest installere disse på alle computere, f.eks. servere og arbejdsstationer, når det vurderes, at rettelserne har positiv indflydelse på den samlede sikkerhed.
Systemejere er ansvarlige for, at der løbende sker regelmæssig opdatering af anvendt software.
IT-afdelingen skal forestå installation af alle større programrettelser, når det vurderes, at disse har positiv indflydelse på den samlede sikkerhed.

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 IT-afdelingen vurdere, om disse skal installeres.
Større opdateringer skal testes i et testmiljø, inden opdateringerne installeres i produktionsmiljøet.

Sikkerhedsopdateringer til netværksudstyr
IT-afdelingen skal dagligt sørge for, at alle benyttede trådløse adgangspunkter og software til disse er opdateret med de seneste sikkerhedsrettelser. Udrulning/installation skal foretages senest 30 dage efter udgivelsen af sikkerhedsrettelsen.

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

Rettelser til applikations-programpakker
IT-afdelingen skal mindst hver uge vurdere tilgængelige sikkerhedsrettelser f.eks. patches eller hot-fixes. Udrulning/installation skal foretages efter behov.

Styring af antivirus
IT-afdelingen 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

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

12.6.2 Begrænsninger på softwareinstallation

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

Administration af softwarelicenser
Registrering af software licenser sker gennem IT-afdelingen. Det er IT-chefens 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
De personer der udfører revisionen, skal være uafhængige af det reviderede område.
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.
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.

13 Kommunikationssikkerhed

13.1 Styring af netværkssikkerhed

13.1.1 Netværksstyring

Indkommende netværksforbindelser
Der må ikke være mulighed for at etablere forbindelser direkte fra internettet til interne systemer.
Der tillades kun etablering af forbindelser fra internet til sikkerhedsgodkendte servere, eksempelvis email- og web-servere.
Forbindelser fra internettet til den demilitariserede netværkszone (DMZ) må kun oprettes til specifikke IP-adresser.

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

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

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

Installation af netværksudstyr
Det er ikke tilladt at installere netværksudstyr uden forudgående sikkerhedsgodkendelse.
Standardværdier, eksempelvis administrator-logins og andre "fabriksindstillinger", skal ændres, før et system installeres på netværket.

Adgang til trådløse netværk for gæster
Gæster, hvis identitet er kendt, kan få udleveret adgangskode til gæstenettet. Ansvarlig mødeleder kontakter IT-servicedesk for nærmere information.

Placering af trådløse netværk
Der er ingen restriktioner på placering af trådløst netværksudstyr.

Adgang til aktive netværksstik
Adgang til aktive netværksstik skal styres af IT-afdelingen.
Ved tilslutning af udstyr til netværksstik i offentligt tilgængelige områder, må der ikke tildeles ip-adresser ved hjælp af DHCP.

Routekontrol
IT-afdelingen skal vedligeholde konfigurationsstandarder for routere.
IT-afdelingen skal sikre passende netværks- eller node-autentificering til ethvert netværkssegment.
IT-afdelingen skal begrænse routning imellem forskellige netværkssegmenter således at kun nødvendig trafik videresendes.

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

Fysisk sikring af netværk
Der skal etableres alternative kommunikationsveje.
IT-afdelingen skal regelmæssigt kontrollere, om uautoriseret udstyr er blevet tilkoblet.
Krydsfelter og kabeltermineringer skal være placeret så fysisk adgang begrænses.

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

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

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

Brug af trådløse lokalnetværk
Brug af trådløse netværk tillades når access pointet befinder sig på et lokalnetværkssegment, der er sikkert adskilt fra sikre lokalnetværkssegmenter (f.eks. ved hjælp af en firewall).

13.1.2 Sikring af netværkstjenester

Fjernstyring og administration
Forbindelser til fjernadgang til brug for leverandører og support, skal overvåges, mens de benyttes.
Det er tilladt at benytte værktøjer til fjernadministration, hvis der foreligger sikkerhedsgodkendelse af produktet.
Adgang til administrations- og konfigurationsporte til trådløse netværk skal begrænses til administratorer.
Værktøjer til fjernadministration tillades, hvis adgangen er krypteret ved hjælp af teknologier som f.eks. SSH, VPN, eller SSL/TLS.

Afvikling af programmer i forbindelse med internetsurfing
Det er tilladt at afvikle browserbaserede programmer, f.eks. netbank-programmer, forudsat at I-sikkerhedspolitikken i øvrigt overholdes.

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

13.1.3 Opdeling af netværk

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

13.2 Informationsoverførsel

13.2.1 Politikker og procedurer for informationsoverførsel

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

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. Der er udarbejdet procedure for lagring og journalisering af fortrolige og følsomme informationer. Proceduren findes på medarbejderweb og i SecureAware.

13.2.2 Aftaler om informationsoverførsel

Udlevering af fortrolige informationer og oplysninger
Fortrolige informationer og oplysninger må udleveres, hvis der foreligger underskrevne fortrolighedsaftaler.
Fortrolig information må ikke udleveres uden forudgående aftale med dokument- eller dataejer.

13.2.3 Elektroniske meddelelser

Ejerskab
Hjørring Kommune betragter alle emails som kommunens ejendom. Medarbejdernes emails er i princippet ukrænkelige. Dette gælder også private emails sendt til og fra en medarbejders arbejdsmail.
Det er acceptabelt at benytte email til private beskeder i rimeligt og begrænset omfang. Private emails skal mærkes privat og eventuelt gemmes i en mappe mærket privat.
Private emails er ikke undtaget fra at kunne åbnes i helt særlige tilfælde, som langvarig sygdom, dødsfald eller mistanke om misbrug af beføjelser. Åbning af medarbejderes emails i ovennævnte tilfælde sker kun efter forudgående underretning af medarbejderen (der skal dog ikke gives samtykke fra medarbejderen) og kun på anmodning fra områdedirektøren eller nærmeste leder alt efter karakteren af behovet for åbning.

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

Opbevaring og sletning af email
Email der indeholder personhenførbare oplysninger, skal behandles i overensstemmelse med persondataloven.
Emails med personhenførbare oplysninger skal journaliseres i SB-sys eller andet relevant fagsystem.
Emails indeholdende personhenførbare oplysninger og som sendes udenfor kommunens netværk skal sendes som sikker eller digital post.
Emails som indeholder aftaler, der forpligter kommunen, skal journaliseres i SB-sys.

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

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

Fortrolig email
Email med følsomt indhold skal krypteres med godkendt software og sendes kun udenfor Hjørring Kommunes netværk ved hjælp af Digital Post eller Doc2mail. Dette gælder både til borgere og virksomheder. Andre offentlige myndigheder vil ofte være tilkoblet tunnelmail. Yderligere information herom findes på medarbejderweb under I-sikkerhed.
Email med følsomt indhold kan sendes sikkert indenfor Hjørring Kommunes netværk uden yderligere kryptering.

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 email, telefon og/eller messenger-programmer.

Vedhæftede filer
Det er tilladt at benytte vedhæftede filer ved brug af email systemet.
IT-afdelingen skal blokere for filtyper som IT-afdelingen vurderer farlige eller uhensigtsmæssige.

Phishing og ransomware
Uanset at kommunen udfører indholdsscanning af alle emails, skal brugere være opmærksomme på "phishing" og "social engineering", der f.eks. kan betyde, at de kan modtage tilsyneladende oprigtige emails, der forsøger at franarre personlige eller fortrolige oplysninger eller forsøger at få brugeren til at foretage uønskede handlinger.
Administrative medarbejdere uddannes løbende i opmærksomhed på phishing og ransomware.

Sagsbehandling og journalisering af email
Sendte og modtagne emails skal håndteres på samme måde som traditionel post og fax. Emails med vigtig information skal arkiveres systematisk for at sikre lagring.
Modtaget og afsendt email skal journaliseres og behandles efter samme principper som gælder for almindelig brevpost og fax.
Hjørring Kommunes emailpolitik og journaliseringsvejledning kan findes i den administrative håndbog på medarbejderweb.

13.2.4 Fortrolighedsaftaler

Indhold af fortrolighedserklæringerne
- Betingelser for returnering eller destruktion af informationsaktiver ved aftalens ophør.
- Underskriverens ansvar for at undgå brud på den aftalte fortrolighed.
- Definition af de informationer, der er omfattet.
- Kommunens ret til overvågning af og opfølgning på overholdelse af fortrolighedspligten.
- Sanktioner ved brud på fortrolighedspligten.

14 Anskaffelse, udvikling og vedligeholdelse af systemer

14.1 Sikkerhedskrav til informationssystemer

14.1.1 Analyse og specifikation af informationssikkerhedskrav

Anskaffelsesprocedurer
Nyanskaffelser må ikke give anledning til konflikt med eksisterende krav i I-sikkerhedspolitikken.
Anskaffelser må ikke give anledning til forøget risiko for sikkerhedshændelser uden forudgående risikovurdering og eventuel detaljeret risikoanalyse.
Anskaffelse af IT-systemer og services skal være i overensstemmelse med I-sikkerhedspolitikken. Hvis det findes nødvendigt, skal der gennemføres risikoanalyse inden anskaffelse.

14.1.2 Sikring af applikationstjenester på offentlige netværk

Sikring af applikationer på offentlige netværk
Der skal benyttes sikre autentifikations- og autorisationsprocesser for at sikre service-transaktioner over offentlige netværk.
Datas integritet og fortrolighed skal sikres, når der benyttes applikations-services over offentlige netværk.
Eksempelvis:
- Integritetssikring (såsom hashing)
- Kryptografiske løsninger (såsom SSL, SFTP, HTTPS, sikre API'er eller webservices)

14.1.3 Beskyttelse af handelsapplikationer og -tjenester

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

14.2 Sikkerhed i udviklings- og hjælpeprocesser

14.2.1 Sikker udviklingspolitik

Sikkerhed i applikationsudvikling
Udviklingsprocessen skal dokumenteres.
Softwareudvikling skal baseres på best practice og indbefatte I-sikkerhed 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.
Der skal genereres log over de aktiviteter, der sender data ind i systemet.

14.2.2 Procedurer for styring af systemændringer

Migreringsstyring
Proceduren for ændringshåndtering skal omfatte test af den operationelle funktionalitet i forbindelse med den enkelte ændring.
Både ny kode og ændringer i eksisterende kode skal gennemgås for sårbarheder.

14.2.3 Teknisk gennemgang af applikationer efter ændring af driftsplatforme

Gennemgang af systemer efter ændringer
Beredskabsplanerne skal tilrettes i overensstemmelse med nye ændringer.
Ændringer i driftsmiljøerne skal annonceres i god tid således, at der er god tid til gennemgang og test inden implementeringen.
Når driftsmiljøerne ændres, skal kritiske forretningssystemer gennemgås og testes for at sikre, at det ikke har utilsigtede afledte virkninger på kommunens daglige drift. Dette er systemejers ansvar.
Når der foretages ændringer af operativsystemer, skal organisationen vurdere behovet for opdatering af beredskabsplanerne.

14.2.4 Begrænsning af ændringer af softwarepakker

Ændringer i standardsystemer
Ændringer i eksternt leverede systemer er kontraktstyret.
Ved systemændringer skal indbyggede sikringstiltag, f.eks. logning samt adgangs- og integritetskontrol, sikres ikke at være kompromitterede.

14.2.5 Principper for udvikling af sikre systemer

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

Specifikation af sikkerhedskrav
Såfremt en overordnet risikovurdering retfærdiggør aktiviteten, skal sikkerhedskrav dokumenteres i forbindelse med enhver IT-system nyanskaffelse eller IT-systemopgradering. Dette gælder både for kundetilpassede- og standardsystemer.

14.2.6 Sikkert udviklingsmiljø

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.

Der skal anvendes en formel livscyklus for systemudvikling, som tager højde for sikkerhed i processen.
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
Kommunen kræver dokumenteret løbende kvalitetssikring.
Kommunen kræver ophavsrettighed på kildekode.
Aftaler om accepttest for kvalitet, nøjagtighed og sikkerhed skal identificeres og være en del af leverancer.
Organisationen skal desuden være i stand til at validere effektiviteten af udviklingsprocesserne.

Ejerskab af data, cloudløsninger
Kommunen skal sikre at ejerskab, herunder regler for ophavsret, kildekode mm. er klart defineret mellem kommunen 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.

14.2.9 Systemgodkendelsestest

Godkendelse af nye eller ændrede systemer
IT-afdelingen 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

Sletning af testdata
Testdata skal fjernes inden systemer sættes i endelig drift.
Særlige applikationskonti, brugernavne og adgangskoder, anvendt i forbindelse med udvikling og test, skal slettes før en applikation sættes i drift eller frigives til kunder.

Sikring af testdata
Det skal formelt godkendes, inden data fra driftsmiljøet kopieres til et testmiljø.
Kopiering og brug af data fra driftsmiljøet til test skal logges for at sikre kontrolsporet.
Data til test skal udvælges, kontrolleres og beskyttes omhyggeligt og i henhold til deres klassifikation.
Formelle adgangskontrolprocedurer skal også omfatte testapplikationssystemer.

15 Leverandørforhold

15.1 I-sikkerhed i leverandørforhold

15.1.1 I-sikkerhedspolitik for leverandørforhold

Vurdering og godkendelse af outsourcingleverandør
IT-afdelingen deltager 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. Sikkerhedsmæssige krav til leverandører sikres i Hjørring Kommunes Kravspec-generator.

Anskaffelse, udvikling og vedligeholdelse ved outsourcing
Systemejer i samarbejde med IT-afdleingen sikrer, at leverandøren har 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 identificeres og aftales med leverandører, der har adgang til, behandler, opbevarer eller leverer IT-infrastruktur til organisationens informationsaktiver.

Misligholdelse, cloudløsning

Kommunen skal sikre, at servicen kan afbrydes i tilfælde af misligholdelse, ved brud på sikkerheden, eller hvis løsningen indebærer en uacceptabel risiko for kommunens informationer og netværk.
Systemejere skal sikre, at der er en "exit-strategi" på plads i tilfælde af misligholdelse.

Kontrakt om cloud-løsning
Aftale med cloud-udbyder sker på grundlag af udbyderens standardkontrakt.
Kommunen skal sikre, at kontrakten som minimum tager højde for de lovgivningsmæssige krav, f.eks. vedr. personoplysninger.
Kommunen skal sikre, at aftalen indeholder væsentlige sikkerhedselementer, såsom roller, opfyldelse af sikkerhedskrav, beredskab, hændelseshåndtering, behandling af data omfattet af lovgivning, brugerstyring, fysisk sikkerhed, beskyttelse af informationer både fysisk og logisk, sletning og udfasning af udstyr og forhold ved aftalens ophør. Dette kan evt. ske via en tillægsaftale.

15.1.3 Forsyningskæde for informations- og kommunikationsteknologi

Netværkssikkerhed, outsourcingleverandør
Leverandøren skal sikre en hensigtsmæssig opbygning af netværk, firewall, segmentering, kryptering mm.
Kommunen skal sikre at leverandørens opbygning af netværk og netværkssikkerhed har et passende sikkerhedsniveau. 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.

Netværksleverandøren skal kunne levere:
- De nødvendige tekniske opsætninger til at sikre opkoblinger i overensstemmelse med samarbejdsaftalen.
- Det nødvendige sikkerhedsniveau i hele leverandør-forsyningskæden.

15.2 Styring af leverandørydelser

15.2.1 Overvågning og gennemgang af leverandørydelser

Overvågning og audit, cloudløsning
Udbyderen skal kunne dokumentere et passende sikkerhedsniveau, eksempelvis revisionserklæring, intern audit, ISO 27001-certificering, outsourcing-revisionserklæring (ISAE16) eller tilsvarende.
Udbyderen skal kunne levere rapportering for, i hvilken grad aftalte servicemål er opfyldt.

15.2.2 Styring af ændringer af leverandørydelser

Styring af ændringer hos serviceleverandøren
Systemejeren sikrer, at ændringsstyring af serviceleverandørens ydelser følger samme retningslinier som kommunens egne.

16 Styring af I-sikkerhedsbrud

16.1 Styring af I-sikkerhedsbrud og forbedringer

16.1.1 Ansvar og procedurer

Ansvar og forretningsgange for sikkerhedshændelser

Ledelsen har fastlagt forretningsgange, der sikrer en hurtig, effektiv og metodisk håndtering af sikkerhedsbrud.

Information om sikkerhedshændelser

I-sikkerhedskoordinator skal jf. gældende procedure informeres om sikkerhedshændelser. Proceduren findes i SecureAware.

Proces for reaktion på hændelser

Processen for styring af sikkerhedshændelser revideres én gang årligt. Proceduren for indrapportering af sikkerhedshændelser findes i SecureAware.

16.1.2 Rapportering af I-sikkerhedshændelser

Sikkerhedshændelser hos outsourcingleverandør

Leverandøren registrerer sikkerhedshændelser, f.eks. brud på fortrolighed, tilgængelighed eller integritet, i eget system.
Leverandøren skal underrette kommunens systemejeren, hvis der sker en sikkerhedshændelse, f.eks. ved brud på fortrolighed, integritet eller tilgængelighed.
Kommunen gennemgår eventuelle sikkerhedshændelser sammen med leverandøren med faste intervaller, eksempelvis på aftalte kontraktmøder.

Rapportering af sikkerhedshændelser

Organisationen og eksterne tjenesteudbydere er forpligtede til at indberette enhver observeret sikkerhedshændelse eller mistanke herom. Til dette følges proceduren i SecureAware. Alle sikkerhedshændelser skal dokumenteres og revideres kvartalsvis i forbindelse med I-sikkerhedsudvalgsmøderne.

Rapportering af formodede sikkerhedshændelser

Ved konstatering af brud eller formodede brud på IT-sikringsforanstaltninger skal rapportering straks ske til IT-supportfunktionen.
Årsager til sikkerhedshændelser bør omfatte:

- 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

Hjørring Kommune kan afbryde for adgangen fra privat udstyr i tilfælde af sikkerhedsbrud, misligholdelse eller hvis det vurderes at udstyret udgør en uacceptabel risiko for kommunens informationer og netværk.

Rapportering af virusangreb

Hvis der observeres virus eller mistanke om virus, skal det omgående rapporteres til IT-afdelingen. PC'en slukkes omgående og afleveres til IT-afdelingen. Kontakt først IT-afdelingen på tlf. 72 33 30 00.

16.1.3 Rapportering af I-sikkerhedssvagheder

Rapportering af programfejl
Brugere der observerer programfejl, skal rapportere dette til systemejeren.

16.1.4 Vurdering af og beslutning om I-sikkerhedshændelser

Vurdering af tidligere hændelser
For at kunne mindske sandsynligheden eller effekten af fremtidige sikkerhedshændelser, skal den forgangne periodes hændelser gennemgås i forbindelse med den kvartalsvise orientering af I-sikkerhedsudvalget.

16.1.5 Håndtering af I-sikkerhedsbrud

Kontrol og opfølgning på sikkerhedsbrud
Brud på sikkerheden, uautoriseret adgang og forsøg på uautoriseret adgang til systemer, informationer og data skal registreres i journalsystemet.
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
- Evt. sanktionsmuligheder.

16.1.6 Erfaring fra I-sikkerhedsbrud

Erfaringer fra sikkerhedsnedbrud
IT-afdelingen skal etablere et system, der kan kvantificere og overvåge typer, omfang og omkostninger ved håndteringen af sikkerhedsbrud. Disse oplysninger skal bruges til at identificere og afbøde tilbagevendende sikkerhedshændelser eller disses konsekvenser.

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.
Det er I-sikkerhedskoordinatoren der er ansvarlig for denne indsamling.

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

17.1 I-sikkerhedskontinuitet

17.1.1 Planlægning af I-sikkerhedskontinuitet

Ramme for beredskabsplaner
Ledelsen 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

IT-afdelingen skal udarbejde og vedligeholde en tværorganisatorisk beredskabsstyringsproces, som skal behandle de krav til I-sikkerhed, der er nødvendige for kommunens fortsatte drift.

17.1.2 Implementering af I-sikkerhedskontinuitet

Beredskabsplan
Beredskabsplan skal foreligge for alle forretningskritiske systemer.

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.

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 I-sikkerhedskontinuiteten

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

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

17.2 Redundans

17.2.1 Tilgængelighed af informationsbehandlingsfaciliteter

Retablering af forretningskritiske systemer på ny lokation
For alle forretningskritiske systemer skal der forefindes en plan for retablering på ny lokation.
Beredskabsplanerne skal afspejle muligheden for, at de fysiske lokationer kan være utilgængelige eller ødelagt.

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 med tilhørende vejledning samt Sikkerhedsbekendtgørelsen gælder ved enhver opbevaring og behandling af persondata.

Der må ikke behandles personoplysninger af fortrolig karakter på privat pc.
Der må ikke behandles personoplysninger af fortrolig karakter på mobilt udstyr, f.eks. bærbar 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 kommunens drift, identificeres.
Status på efterlevelsen af love og regler inden for IT-området skal monitoreres løbende og revideres mindst en gang hvert år.

Retningslinier for ophavsrettigheder
IT-afdelingen skal løbende kontrollere, at software-licensaftaler overholdes, f.eks. at eventuelle begrænsninger i antal brugere, servere eller kopier overholdes.
IT-afdelingen skal løbende kontrollere, at der kun er installeret autoriserede systemer med autoriserede licenser i kommunen.

18.1.3 Beskyttelse af registreringer

Lagring og adgangsrettigheder til systemdokumentation
Systemdokumentation opbevares i mindst 3 år.

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

Sikring af kommunens lovbestemte data
Kommunens 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
Kommunen skal sikre at personoplysninger behandles loyalt, lovligt og på en gennemsigtig måde for den registrerede.
Kommunen må indsamle personoplysninger til udtrykkeligt angivne og legitime formål.
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
Den registreringsansvarlige skal hurtigst muligt efter et brud på persondatasikkerheden, foretage anmeldelse til tilsynsmyndigheden.
Anmeldelse skal blandt andet beskrive bruddets art, karakteren af bruddet på persondatasikkerheden, konsekvenser og afhjælpende foranstaltninger.

Der er udarbejdet vejledning, procedurebeskrivelse og kommunikationsplan til sikring af overholdelse af 72-timers fristen.

Registerfører for personoplysninger
Hvis en behandlingsaktivitet foretages på vegne af en virksomhed skal der vælges en registerfører.

Forudgående godkendelse og høring for behandling af personoplysninger
Kommunen (den registeransvarlige) eller registerføreren skal indhente godkendelse fra tilsyns-myndigheden inden behandlingen af personoplysninger.

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

Databeskyttelse af personoplysninger
Kommunen skal gennemføre mekanismer med henblik på at sikre, at kun de personoplysninger, der er nødvendige til det specifikke formål med behandlingen, behandles.

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

Udpegning af den databeskyttelsesansvarlige for personoplysninger
Kommunen skal udpege en databeskyttelsesansvarlig, når behandlingen foretages af en virksomhed, der beskæftiger mindst 250 personer.

18.1.5 Regulering af kryptografi

Regulering på kryptografiområdet
Kommunen skal efterleve nationale regler for kryptering. Dette gælder også for medarbejdere, der besøger andre lande, medbringende bærbart og mobilt udstyr. Juridisk afdeling og den sikkerhedsansvarlige er ansvarlig for at informere medarbejdere om de regler og retningslinier, der er gældende.

18.2 Gennemgang af I-sikkerhed

18.2.1 Uafhængig gennemgang af I-sikkerhed

Uafhængig audit af I-sikkerheden
Kommunens ISMS skal være underlagt en, for IT-sikkerhedsafdelingen, uafhængig audit.
Audit skal omfatte:

- I-sikkerhedspolitik
- IT-sikkerhedsregler - og disses efterlevelse
- IT-sikkerhedsprocedurer
- ISMS processer.

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

Audit foretages af I-sikkerhedskoordinator.

Overvågning og audit af outsourcingleverandør
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.
Periodiske service-statusmøder skal omhandle sikkerhedsrelaterede emner såsom sikkerhedshændelser og resultater af KPI'er.

18.2.2 Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder

Revision af I-sikkerhedspolitik
Den interne audit skal kontrollere, at I-sikkerhedspolitikken er velimplementeret i organisationen og overholdes. Denne audit skal foretages en gang om året, og audit bør omfatte beskrivelse af årsagen til afvigelser, handlingsplaner, der er nødvendige for at håndtere afvigelserne (korrigerende handlinger) samt en efterfølgende vurdering af effektiviteten af de foranstaltninger, der gennemføres.

Intern audit foretages af I-sikkerhedsadministrationen.

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.