Overskrift

Indledning og formål

Formål med dette afsnit

Afsnittet giver en generel beskrivelse af baggrunden for udarbejdelse af sikkerhedshåndbogen - for at sikre, at det er klart, hvilke områder håndbogen behandler (og hvilke der ikke behandles).

Ansvarlig for område

IT-sikkerhedsgruppen

Afsnit sidst revideret

25.11.2015 - aviln

Beskrivelse

IT-Sikkerhedshåndbogen beskriver håndtering af IT-sikkerheden i Gribskov Kommune og fastsætter krav og forventninger til kommunens IT-sikkerhed.

Med IT-sikkerhed menes i denne sammenhæng følgende 3 hovedpunkter:

- Sikkerhed for driften af kommunens IT-systemer og dermed adgang til komplette informationer og rutiner heri, således at kommunens personale på bedste vis uhindret kan planlægge og udføre deres daglige arbejde, som afhænger af disse systemer. Herunder også nødplaner for drift i tilfælde af særlige problemer.
- Sikkerhed for, at fortrolige oplysninger fra Gribskov Kommunes systemer ikke havner hos trediepart, som ikke har berettiget adkomst til disse informationer. Dette sker dobbelt dels via konkret adgangskontrol og dels ved sikring af korrekt omgang med informationerne fra de ansattes side. Dette gælder i forhold til parter helt udenfor kommunens medarbejderkreds, men også internt så den enkelte medarbejder begrænser sin tilgang til de fortrolige informationer, der er behov for i forbindelse med varetagelsen af egne opgaver.
- Sikkerhed for, at øvrig lovgivning, som omhandler anvendelse af informationsteknologi, overholdes af kommunens medarbejdere i udførelse af deres arbejde.

IT-sikkerhedshåndbogen, udgør sammen med IT-sikkerhedspolitikken (bilag 1) kommunens overordnede IT-sikkerhedsregler.

IT-sikkerhedshåndbogen beskriver de generelle rammer for tiltag, kommunikation og ansvar omkring sikkerheden.

Som et led i den overordnede sikkerhedsstyring tager ledelsen på grundlag af den løbende overvågning og rapportering sikkerhedshåndbogen op til revurdering én gang om året.

Der er særligt lagt vægt på persondataloven med bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (bilag 2), samt på forvaltningslovens § 32 (bilag 3).

Formål
Informationer og informationssystemer har altafgørende betydning for Gribskov Kommune, og informationssikkerheden har derfor vital betydning for kommunens troværdighed og funktionsdygtighed.

Formålet med IT-sikkerhedshåndbogen er at definere en ramme for beskyttelse af virksomhedens informationer og særligt at sikre, at kritiske og følsomme informationer og informationssystemer bevarer deres fortrolighed, integritet og tilgængelighed.

Derfor har Gribskov Kommunes ledelse besluttet sig for et beskyttelsesniveau, der er afstemt efter risiko og væsentlighed samt overholder lovkrav og indgåede aftaler, herunder licensbetingelser.

Ledelsen vil med IT-sikkerhedshåndbogen oplyse medarbejderne om ansvar i relation til virksomhedens informationer og informationssystemer.

Hensigten med IT-sikkerhedshåndbogen er endvidere at tilkendegive over for alle, som har relation til kommunen, at anvendelse af informationer og informationssystemer er underkastet standarder og retningslinier.

På den måde kan sikkerhedsproblemer forebygges, eventuelle skader kan begrænses, og reetablering af informationer kan sikres.

Tiltag: Check af sikkerhedsrutiner
Frekvens: Jvf. sikkerheds årshjul (årligt)
Ansvar: Den overordnede sikkerhedsansvarlige
Kommunikation: Resultat meldes ud i organisationen og eventuelle opfølgningspunkter afrapporteres efterhånden som de afklares/løses.

Som et led i den overordnede sikkerhedsstyring tager ledelsen på grundlag af den løbende overvågning og rapportering sikkerhedspolitikken op til revurdering én gang om året.

Overskrift

Organisering og ansvar

Formål med dette afsnit

For klart at sikre, at alle relevante aspekter og opgaver i relation til IT-sikkerheden varetages, udpeges ansvarlige for de enkelte emner, de enkelte tiltag og de enkelte beskrivende dokumenter.

Ansvarlig for område

IT-sikkerhedsgruppen

Afsnit sidst revideret - dato og navn

25.11.2015 - aviln

Beskrivelse

Ansvarsdefinitioner i sikkerhedshåndbogen ligger hos navngivne roller/stillinger i organisationen og dermed via deres "kasket" hos navngivne enkeltpersoner i den enkelte situation.

Visse ansvarsdefinitioner ligger hos én personlig "kasket" eller rolle - dvs. ansvaret påhviler én enkelt person, fx. "Leder af IT-drift". Andre ansvarsdefinitioner ligger hos en gruppe-rolle - dvs. ansvaret påhviler en gruppe, men i den enkelte situation alligevel altid én enkelt person, fx. "Område-chefen" eller "Den system-ansvarlige".

For at sikre kobling mellem roller og navngivne personer på et givent tidspunkt i en given situation henvises til bilag: "Liste over roller og navngivne personer" (bilag 4).

- Alle emner beskrevet i Sikkerhedshåndbogen har én udpeget ansvarlig
- Alle bilag beskrevet i Sikkerhedshåndbogen har én udpeget ansvarlig
- Alle tiltag beskrevet i Sikkerhedshåndbogen har én udpeget ansvarlig

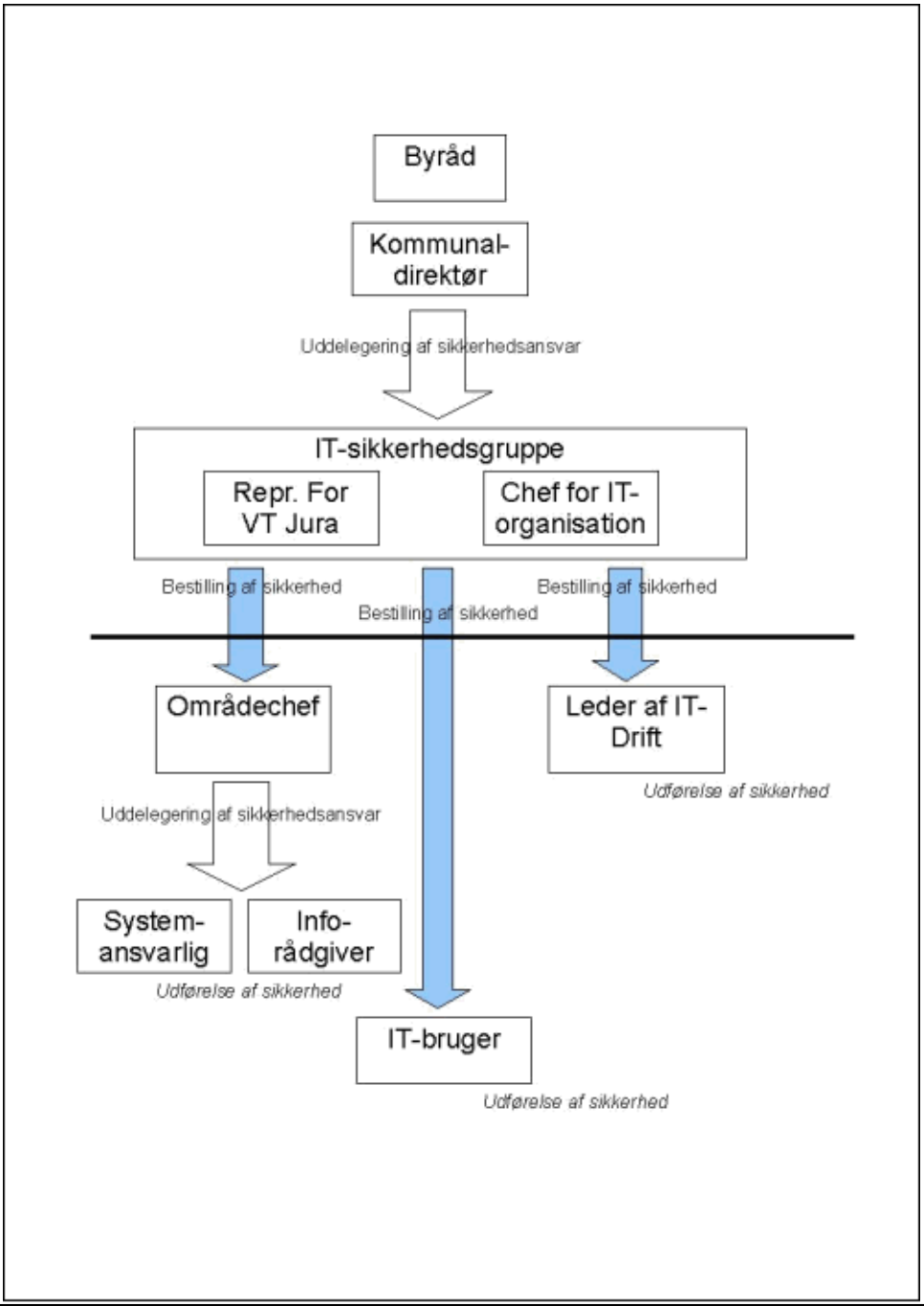
Som hovedregel gælder følgende princip:

- IT-sikkerhedsgruppen er overordnet sikkerhedsansvarlig og kan uddelegere sine konkrete opgaver i den sammenhæng. Som sådan er denne gruppe bestiller af sikkerhed på IT-området.
- Ansvaret for udførelse af sikkerheden omkring de tekniske, driftsmæssige og IT-adgangskontrolmæssige forhold påhviler typisk lederen af IT-drift.
- Overholdelse af sikkerhedsmæssige forhold omkring den enkelte medarbejders anvendelse af IT-systemer og informationer påhviler den enkelte medarbejder selv. Det er således den enkelte medarbejder, der er udfører. Dog gælder det forhold, at chefen for området indledningsvis skal sørge for, at de relevante regler og retningslinier er den enkelte medarbejder bekendt. Info-rådgiverne kan inddrages i dette arbejde.
- Hvert system er knyttet til et område. Hvis der er tale om et ikke-område-specifikt system er dette område IT-organisationen. Den ansvarlige chef for området uddelegerer systemansvar til en systemansvarlig.

Arbejdet omkring sikkerhed er bygget op omkring Gribskov Kommunes IT-systemer og de informationer, der behandles i dem. Det foregår typisk omkring én af følgende slags begivenheder:

- Årligt check af sikkerhedsrutiner og tiltag - særligt beskrevet i følgende: (bilag 5)).
- Indførelse af ny software eller anden form for teknologi - særligt beskrevet i de enkelte emner/afsnit i Sikkerhedshåndbogen
- Ansættelse af nye medarbejdere - særligt beskrevet i afsnit om medarbejdersikkerhed: (bilag 6).
- Indtræden af sikkerhedsmæssig hændelse - defineret som driftsforstyrrelse eller overtrædelse af sikkerhedsregler - nærmere beskrevet i de enkelte emner/afsnit i Sikkerhedshåndbogen.

Sikkerhedsstrukturen ses her:



Overskrift

Driftsikkerhed

Formål med dette afsnit

Ud fra nedenstående beskrives de forhold, der er gældende for Gribskov Kommune for så vidt angår data - og driftsikkerhed

Ansvarlig for område

Chefen for IT-organisationen

Afsnit sidst revideret - dato og navn

25.11.2015 - brasm

Beskrivelse

Driftsikkerhed

Dette afsnit beskriver de vurderinger, der skal foretages på følgende områder:

1. Den generelle opbygning af IT miljøet.
2 .Den samlede vigtighed for de enkelte IT-systemers afvikling i forhold til organisationens samlede virke.
3. Den fysiske infrastrukturs opbygning og valg af teknologi.
4. Backup strategi.
5. Restore strategi.
6. Patch management.
7. Trafik screening.
8. Virusbeskyttelse.

Tiltag: Check af sikkerhedsrutiner.
Frekvens: Jvf. sikkerheds årshjul (årligt).
Ansvar: Den overordnede sikkerhedsansvarlige.
Kommunikation: Resultat meldes ud i organisationen og eventuelle opfølgningspunkter afrapporteres efterhånden som de afklares/løses.

Driftsikkerhed

1. Opbygning af IT miljø
Ved valg af IT miljøet for Gribskov Kommune blev det besluttet, at alle vigtige IT-systemer, der havde direkte betydning for enten driftsikkerheden, eller tilgængeligheden for brugernes anvendelse og kundebetjening, skulle afvikles i en sådan forstand, at data m.v. i videst mulig omfang var tilgængelig hele tiden. Dette er sikret ved, at alle primære IT-systemer afvikles i et miljø, hvor dublering og systembackup er anvendt.

2. De enkelte IT systemers vigtighed i forhold til organisationens virke.
Ud fra en vurdering om vigtigheden af tilgængeligheden af hensyn til borgernes betjening skal de primære IT-systemer være dubleret, eller der skal anvendes system-backup.

Af systemtekniske årsager kan der være systemer, hvor det enten ikke er muligt eller rentabelt at foretage dublering. For en samlet liste over disse systemer og vurderingen af deres vigtighed (bilag 7 .

3. Fysisk infrastruktur og teknologivalg.

Alle primære lokationer i Gribskov Kommune skal forbindes ved en teknologi, der sikrer, at der er kapacitet nok til, at medarbejderne kan udføre deres arbejde på en tilfredsstillende måde. Typen af forbindelse afgøres ud fra vigtigheden af den givne lokation samt behovet for transmissionshastighed og datamængde. Den anvendte teknologi til datatransmission skal være baseret på internationale standarder, hvortil der frit kan vælges mellem leverandører og producenter.

I forbindelse med placering af aktivt netværksudstyr skal det sikres, at 3. part ikke kan opnå fysisk adgang til disse. Det skal ligeledes tilses, at der ikke i umiddelbar nærhed af aktivt netværksudstyr forefindes vandrør samt andre fysiske installationer, der kan påvirke datatransmissionen.

Trådløst netværk skal være beskyttet af en anerkendt krypteringsalgoritme.

For beskrivelse af anvendt udstyr og løsninger (bilag 8).

4. Backup
Der skal være en beskrevet backup politik, der skal sikre et defineret antal generation af backup. IT udstyr, der foretager backup af drift systemer, skal være placeret på en anden lokation, end den der anvendes til driften af Gribskov Kommunes primære IT systemer.

Der skal foretages kvartalvis kvalitetskontrol af foretaget backup. Den kvartalsvise kontrol foretages af den sikkerhedsansvarlige i Gribskov Kommune. Bilag 7 for beskrivelse af back-up mv. for de enkelte systemer og bilag 9 for beskrivelse af backup-politik.

5. Restore
Der skal være en beskreven restore-politik, der sikrer en entydig fremgangsmåde i en restore-situation. Der skal 2 gange årligt foretages en test af Gribskov Kommunes data-restore-funktionalitet. Dette foretages ved, *at den sikkerhedsansvarlige* udvælger 2 tilfældige områder, der efterfølgende reetableres på et system holdt uden for den daglige drift, hvorved datas validitet kontrolleres. Oplysning om resultatet af disse kontroller forelægges af den sikkerhedsansvarlige for IT-sikkerhedsgruppen. Se bilag 10 for beskrivelse af restore-politik.

6. Patchmanagement
Alle IT systemer skal løbende vedligeholdes med sikkerhedsopdateringer. Alle primære IT systemer skal løbende vedligeholdes i overensstemmelse med god skik. Det skal ligeledes tilses, at drivere og andet nødvendigt af teknologisk tilsnit løbende holdes opdateret for at optimere driftsikkerheden. For beskrivelse af den valgte løsning (se bilag 11).

7. Trafik screening
For at sikre Gribskov Kommunes IT-systemer kan der foretages en screening af trafik genereret af enheder, der anvender Gribskov Kommunes netværk. Det skal sikres, at adgang til IT-systemer i Gribskov Kommune valideres mod en aktiv brugerdatabase. Endvidere skal det sikres, at datatransmissionen mellem fjernarbejdspladsen og IT systemerne i Gribskov Kommune er beskyttet ved hjælp af en international anerkendt algoritme.

8. Virusbeskyttelse
Der anvendes et internationalt anerkendt antivirus produkt. Dette er installeret på servere og pc'ere.

Overskrift

Nødberedskab

Formål med dette afsnit

Formålet med dette afsnit er at tilkendegive, hvilke emner der i forbindelse med udarbejdelse af dette afsnit, skal medtages.

Ansvarlig for område

Lederen af IT-Drift

Afsnit sidst revideret - dato og navn

25.11.2015 - holse

Beskrivelse

Med dette afsnit angives det , at der på væsentlige områder er foretaget en afvejning af nødvendigheden for virksomhedens daglige afvikling i forhold til IT anvendelsen.

For så vidt angår et generelt nødberedskab i Gribskov Kommune skal alle virksomhedsområder selvstændigt udarbejde procedurer, der gør, at den daglige arbejdsgang uhindret kan udføres i det tilfælde, at IT systemerne i en kortere eller længere periode ikke er tilgængeligt (se bilag 12).

Ud over dette afdækkes i bilagsform de områder, hvor det ud fra en rimelig betragtning er muligt at opbygge et teknologisk nødberedskab samt en kort beskrivelse af de løsninger, der er anvendt (se bilag 13).

Sikkerhedshåndbog for Gribskov Kommune

Overskrift

Fysisk sikkerhed - opbevaring af informationer etc.

Formål med dette afsnit

Afsnittet beskriver og giver overordnede retningslinier for de basale fysiske og omgivelsesmæssige krav omkring den fysiske sikkerhed i organisationen.

Ansvarlig for område

Intern Service, Bygningstjenesten, samt lederen for IT-Drift

Afsnit sidst revideret - dato og navn

25.11.2015 - mptop

Beskrivelse

Det følger af § 5 i bekendtgørelse om sikkerhedsforanstaltninger, at den dataansvarlige myndighed skal fastsætte nærmere interne bestemmelser om sikkerhedsforanstaltninger i myndigheden til uddybning af de regler, der fremgår af bekendtgørelsen. Bestemmelserne skal navnlig omfatte organisatoriske forhold og fysisk sikring, herunder sikkerhedsorganisation, administration af adgangskontrolordninger og autorisationsordninger samt kontrol med autorisationer.

Emnerne i denne beskrivelse er følgende:

- IT-installationens fysiske og geografiske placering (Bilag 14)
- Naboers betydning (Bilag 15).
- Sektionering af bygningen og dens rumopdeling (Bilag 16).
- Opbygning og beskyttelse af tekniske installationer og sikringsanlæg (Bilag 17).
- Fysisk adgangskontrol (Bilag 18).
- Fjernelse af IT-udstyr (se herunder.)
- Mekanisk og teknisk sikring af rum (Bilag 19).
- Kabelinstallationer (se herunder).
- Vandinstallationer (se herunder).
- Offentlig elforsyning og nødstrøm (se herunder).
- Ventilation og kølingsanlæg (se herunder).
- Brandslukningsanlæg (se herunder).
- Overvågning af de tekniske anlæg og installationer herunder varsling (se herunder)

I dette afsnit opstilles der nogle overordnede generelle retningslinier og forslag til den fysiske sikkerhed til både bygninger og IT-koncepter.

De opstillede retningslinier skal i hvert enkelt tilfælde afstemmes i forhold til konceptets kompleksitet og de til konceptet hørende registres sensitivitet dvs. personfølsomhed.

Det skal nævnes, at en IT-installation's fysiske og geografiske placering i mange tilfælde kan være givet på forhånd. Men i andre tilfælde kan den mere frit vælges ud fra en idealsituation. Bilag om IT-installationens fysiske og geografiske placering ses her (bilag 14). Bilag om naboers betydning ses her (bilag 15).

Generelt skal der i alle tilfælde ved indretning af serverrum og andre rum, hvori der skal installeres IT-udstyr og servere tages hensyn til og overvejelser omkring de muligheder for skader, der kan opstå. Der kan fx opstå skader ved afbrydelse af strømforsyning og telefonforbindelser samt andre eksterne forbindelser i form af WAN- og fiberforbindelser. Der kan ske vandskader fx oversvømmelser, brand og røgskade. Endvidere kan der ske "menneskeskabte" ulykker, som fx indbrud, hærværk, tyveri samt sikkerhedstrusler.

Det påhviler den enkelte ansvarlige person at kontakte den sikkerhedsansvarlige for at opnå fornøden sikkerhedsmæssig godkendelse af, at den fysiske sikkerhed kan godkendes. En sådan godkendelse udstedes skriftligt af sikkerhedsansvarlig.

Sektionering af bygningen og dens rumopdeling

Gribskov Kommune har opdelt bygningerne i tre zoner, hvor der er forskellige sikkerhedsforanstaltninger gældende. Zonerne, Rød, Orange og Grøn er beskrevet som følgende:

Rød Zone

Den røde zone omfatter områder, hvor der foretages databehandling af informationer med sensitive oplysninger, serverrum og kontorer med

enkeltstående PC'ere indeholdende sensitive data. I Gribskov Kommune er der ikke pc'ere, som benyttes til dataopbevaring, og dermed er det kun serverrummet og hovedkrydsfelterne, som er omfattet af denne zone.

I serverrummet er der kun adgang for personer med adgangstilladelse udstedt af data-sikkerhedsansvarlig. Det er medarbejdere i IT-driftfunktionen, som har fået udstedt adgangstilladelse til denne zone. Det betyder også, at der ikke må være andre alene tilstede i rum i denne zone uden opsyn af en IT-medarbejder.

Nøgler til serverrum er udleveret til ansatte i IT-drift. Liste over personer med nøgler forefindes i Direktionssekretariatet.

Der er eksterne samarbejdspartnere med nøgle til serverrum med hensyn til sikkerhedsforanstaltninger i tilfælde af indbrud, brand eller lignende.

- Vagtselskab
- Brandvæsen v/Falck A/S
- CL Electric

Orange Zone

Den orange zone omfatter områder, hvor der arkiveres lagringsmedier indeholdende informationer med sensitive oplysninger dvs Back-up rum og arkiver. Andre områder, hvor arkiverne indeholder sensitive data, er aflåst og medarbejderne har kun adgang i forbindelse med deres almindelige arbejde.

Grøn Zone

Zoner hvor informationer med sensitive oplysninger kun opbevares og anvendes i begrænset omfang, dvs kontorer med PC/terminal tilsluttet netværk, er sikkerhedszone Grøn. I denne zone er der kun adgang for Gribskov Kommunes medarbejdere og eksterne personer i følge med medarbejdere. Alle rum, som ikke er omfattet af sikkerhedszone Rød eller Orange, er klassificeret som Grøn. Rum, hvor der ikke er IT-adgang eller arkivadgang, er ikke omfattet.

Yderligere detaljer omkring zoneopdeling mv. er beskrevet i bilag: Sektionering af bygningen og dens rumopdeling (se bilag 16).

Fjernelse af IT-udstyr

Alt IT-udstyr bliver bortskaffet under hensyntagen til de regler, som er gældende med hensyn til miljølovgivning. Alt IT-udstyr herunder også medier m.m. bortskaffes på en sådan måde, at der ikke kan opstå situationer, hvor andre kan anvende sensitive data, som ligger på disse, eller kan få adgang til IT-systemerne. Det er IT-organisationens ansvar - hvis der er begrundet mistanke om, at dette er muligt på et givet system, som skal bortskaffes - at sørge for at dette bliver ødelagt, således at dette ikke kan ske.

Kabelinstallationer
Alle servere er via el-udtag tilsluttet særskilt el-gruppe i el-tavler. Gruppetavlerne er korrekt galvanisk jordet. Grupperne er opsat af autoriserede elektrikere, og via UPS anlæg sikret mod fejl- og overspænding. Centrale enheder skal transcient sikres.

Vandinstallationer
Der er ingen primære vandinstallationer i lokaler, der anvendes til centralt IT

udstyr.

Offentlig elforsyning og nødstrøm
Ud over den offentlige strømforsyning, er der etableret UPS anlæg i forbindelse med centralt IT udstyr.
På lokationer, der fungerer for relæstationer i den primære infrastruktur, anvendes ikke elektronisk udstyr i forbindelse med videre transmission af datasignaler.

Ventilation og kølingsanlæg
Der er etableret et kølingsanlæg i server- og UPS-rum. Kapaciteten af køleanlægget er dimensioneret således, at der i varme perioder kan opretholdes det korrekte temperatur-interval. Køleanlægget vil via alarmordningen give varsling om, at temperaturen stiger over det tilladelige. Samtidig er alarmordningen tilsluttet en ekstern alarmcentral

Brandslukningsanlæg
Der er etableret automatisk brandslukningsudstyr.

Overvågning af de tekniske anlæg og installationer, herunder varsling
Der er etableret overvågning af de centrale IT systemer, hvorved der kan udtages information til brug for varsling.

Overskrift

Systemmæssige forhold

Formål med dette afsnit
Beskrivelse af sikkerhed ifm. systemmæssige forhold

Ansvarlig for område
Lederen af IT-Drift

Afsnit sidst revideret - dato og navn
25.11.2015 - aviln

Beskrivelse
Dette afsnit beskriver forhold omkring:

1. Softwarelicenser

Gribskov Kommune anvender primært ulicenserede kontorprogrammer anvendt under regler for GNU, Open source.

Øvrige primære IT systemer er licenserede, og der er indgået vedligeholdelsesaftaler på de fleste områder for at sikre den foretagede investering.

Der lægges stor vægt på, at enhver anvendelse af software sker under overholdelse af gældende love og producenternes licensbetingelser.

Der må under ingen omstændigheder på nogen computer i kommunen anvendes programmer/systemer, hvortil der ikke er erhvervet en lovlig licens eller tilladelse.

Al installeret software skal være godkendt af GK.

Kopiering af software er kun tilladt i det omfang, det fremgår af licensbetingelserne eller af særlige tilladelser fra producenterne.

Bilag 20.

2. Sikkerhedspakke

Der skal været implementeret sikkerhedspakker på alle enheder i Gribskov Kommune.

Når der kommer nye opdateringer til programmellet, skal disse opdateringer umiddelbart og inden 3 arbejdsdage være implementeret på alle enheder.

Bilag 21.

3. Andre forhold omkring medarbejdernes anvendelse af Gribskov Kommunes IT systemer

Bilag 22.

4. Administrative brugernavne, samt håndtering af eksterne leverandører

Bilag 23.

5. Dokumentation

Bilag 24.

Overskrift

Datasikkerhed

Formål med dette afsnit

Formålet er at beskrive hvilke vurderinger der er foretage f.s.v.a. datasikkerhed, samt beskrive regler herfor.

Ansvarlig for område

IT-Chefen

Afsnit sidst revideret - dato og navn

25.11.2015 - aviln

Beskrivelse

Det følger af § 5 i bekendtgørelse om sikkerhedsforanstaltninger, at der skal fastsættes instrukser, som fastlægger ansvaret for og beskriver behandling og destruktion af ind- og uddatamateriale samt anvendelse af edb-udstyr.

I dette afsnit beskrives følgende:

1. Definitionen af data
2. Medarbejderes forpligtelse i forhold til håndtering af data
3. Opbevaring og håndtering af digitale medier
4. Opbevaring og håndtering af analoge medier
5. Bortskaffelse af data
6. Forhold omkring inddata
7. Dataoverførelser
8. Firewall
9. Medarbejdernes anvendelse af email og internet.
10. Anvendelse af Digital signatur

Datasikkerhed

1. Definitionen af data

Definition af data er i denne forbindelse et hvert form for medie, hvor det er muligt at lagre information på.

Medarbejdere i Gribskov Kommune skal i al enkelthed i deres daglige arbejde overholde de retningslinier, der er udstukket i Loven om Persondata.

Derudover skal medarbejdere i Gribskov Kommune via deres håndtering af datamedie sikre, at intet medie, digitalt eller analogt, bevist eller ubevist, kan komme 3. part i hænde.

I det følgende er Gribskov Kommunes gældende regler beskrevet.

2. Medarbejderes forpligtelse

Der må ikke gemmes data indeholdende personidentificerbare oplysninger lokalt på pc'ers harddisk.
Der må ikke gemmes data indeholdende personidentificerbare oplysninger på håndbårne terminaler.
Mails med personidentificerbare oplysninger, der sendes eksternt må kun sendes krypteret.

3. Digitale medier

Digitale medier, CD, DVD, USB-nøgler etc. indeholdende personidentificerbare oplysninger må kun anvendes og opbevares på en af Gribskov Kommunes lokationer. Digitale medier må ikke afsendes med almindelig post. Digitale medier skal til enhver tid opbevares på en sådan måde, at ingen 3. part bevidst eller ubevidst kan opnå adgang til disse. Medarbejdere er forpligtet til ved arbejdstids ophør at sikre, at digitale medier opbevares forsvarligt i fx en aflåst skuffe eller et arkivrum.

Medtages digitale medier uden for en af Gribskov Kommunes lokationer, er det medarbejderens forpligtelse at sikre, at data er krypteret efter en gældende metode.

Rundsendelse af digitale medier mellem Gribskov Kommunes lokationer må kun foretages af medarbejdere i Gribskov Kommune under forudsætning af, at punkt 5 overholdes.

Medarbejdere skal i forbindelse med anvendelse af Gribskov Kommunes IT systemer særligt iagttage den valgte anvendelse af offentlighedens tilgang til informationer. Det betyder, at navne, initialer samt cpr numre ikke må medtages i mødereferater og andre sager af mere almen karakter.

4. Print og andre analoge medier

Medarbejdere skal sikre, at 3. part ikke bevidst eller ubevist kan opnå mulighed for at læse og håndtere sager med personidentificerbare oplysninger.

Medarbejderen skal sikre, at personidentificerbare oplysninger der udprintes afhentes hurtigst muligt og ikke ligger uovervågede og tilgængelige i printernes papirbakker. Ligeledes skal medarbejdere sikre, at udprintet materiale, der indeholder personidentificerbare oplysninger, bortskaffes på en forsvarlig måde.

Ved transport af papirer indeholdende personidentificerbare oplysninger skal den

enkelte medarbejdere sikre sig, at dette sker på en forsvarlig måde, så 3. part ikke på nogen måde kan opnå fysisk adgang til materialet.

5. Bortskaffelse
Papir med personidentificerbare oplysninger må under ingen omstændigheder bortskaffes via en medarbejders private affaldssystem.

Gribskov Kommune har på de største lokationer opsat beholdere til indsamling af materiale til makulering.

Medarbejdere på mindre lokationer, er forpligtet til at indsamle papirmateriale med person-identificerbare oplysninger og på en forsvarlig måde sørge for, at materiale makuleres efter gældende forskrifter.

Beholdere indeholdende materiale til makulering tømmes jævnligt og opbevares forsvarligt i et dertil specificeret aflåst rum.

6. Inddata
Inddatering til de enkelte systemer må kun foretages af de medarbejdere, som er bemyndiget af systemansvarlig til det.

Ved inddatering til on-line systemer skal der foretages visuel kontrol af indtastede oplysninger på skærmbilledet. Konstaterede fejlregistreringer skal hurtigst muligt slettes eller straks rettes ved indberetning til systemet.

Inddateringen til de enkelte systemer må kun foretages af de personer, der er bemyndiget hertil i forbindelse med anvendelse af det pågældende system.

For systemer hvor der fx ikke i kasse- og regnskabsregulativet eller i forskrifterne er anført særlige instrukser, er områdechefen eller systemansvarlig ansvarlig for at foretage den fornødne bemyndigelse.

Eventuelt inddateringsmateriale skal, når det ikke benyttes, opbevares aflåst.

Det er systemansvarliges ansvar, at der kun udleveres nøgler i overensstemmelse med den gældende kontrolinstruks.

Med mindre det af aftalespecifikationen fremgår, at servicebureauet tilintetgør inddatamaterialet efter endt brug, er det systemansvarlig eller virksomhedslederens ansvar, at inddatamaterialet tilintetgøres indenfor den i de uddybende regler for det pågældende system fastsatte kassationsfrist.

Rekvirering af udskrifter

Den person, til hvem uddata er adresseret, skal kontrollere, at de fastsatte leveringstidspunkter i driftsplanen overholdes. Dette gælder uanset om udskrifterne fysisk sendes eller direkte sendes til udskrift på en lokal stående printer i organisationen.

Hvis ikke leveringstidspunktet overholdes, skal denne person rette henvendelse til IT-centralens sikkerhedsansvarlige og underrette systemansvarlig eller områdechefen.

Udskrivning udenfor driftsplanen kan kun ske efter en skriftlig rekvisition fra en medarbejder, der efter indstilling fra systemansvarlig eller af områdechefen er bemyndiget hertil.

Når en af systemansvarlig eller data-sikkerhedsansvarlig bemyndiget medarbejders ansættelsesforhold ophører eller ændres, så medarbejderen ikke længere varetager de funktioner, der begrundede bemyndigelsen, skal data-sikkerhedsansvarlig underrettes.

Udskrifter fremsendes fra IT-bureauerne i henhold til de gældende driftsplaner

eller i henhold til særlige aftaler og aftalespecifikationer.

Derudover må udskrifter kun rekvireres i overensstemmelse med de for hvert system indgåede driftsaftaler med tilhørende aftalespecifikationer, (jf. de systemspecifikke bilag).

Bestemmelser vedrørende rekvisition af udskrifter vedrører i almindelighed kun udskrifter med oplysninger, der kan henføres til bestemte personer.

I særlige tilfælde kan der for visse registre ske telefoniske bestillinger af uddata. Der er i såfald fastsat særlige regler for det i aftalerne med servicebureauet.

Rekvirering af udskrifter fra specielt Kommunedata A/S edb-centraler må kun foretages i henhold til aftalespecifikationen for det pågældende system.

Rekvirering af udskrifter fra andre centrale IT-systemer, der afvikles på servicebureauer, må kun foretages af medarbejdere, som er bemyndiget til det af systemansvarlig.

7. Dataoverførelser
Kun IT organisationens ledelse kan beslutte, at der oprettes en forbindelse der muliggør automatisk overførelse af data til 3. parts IT-systemer.

Kun IT organisationens ledelse kan beslutte overførelse af data til et givet IT-system afviklet i Gribskov Kommunes regi.

Der skal foreligge en tydelig snitfladebeskrivelse, inden en godkendelsesproces kan i gang sættes.

Der udarbejdes og vedligeholdes løbende et katalog, der beskriver hvilke IT systemer, der automatisk udveksler beskrevne data med 3. parts IT-systemer.

Der foretages intern revision af dette katalog.
Den interne revision udføres af den IT-sikkerhedsgruppen i Gribskov Kommune.

8. **Firewall**
Der skal være installeret en sikkerhedsforanstaltning (firewall), der regulerer trafik til og fra internet.

Forsøg på uautoriseret brug og adgang til firewall'en logges og udløser alarmer. Firewall-installationen skal løbende vedligeholdes i takt med fremkomsten af stadig flere risici.

9. **Medarbejdernes anvendelse af Internet og email**

Internettet må benyttes af alle til tjenstlige formål.

Retningslinjer for håndtering af internet og email fremgår af bilag 22.

Medarbejderne kan anvende internet og mail til private formål, det skal klart fremgår hvis mail har privat karakter. Dette sker under hensyntagen til den fleksibilitet der er i at kunne tage udstyr (bærbar pc) med hjem.

Af sikkerhedsmæssige hensyn screenes der overordnet på mailtrafik ind/ud af Gribskov Kommunes mailserver.

10: Anvendelse af medarbejder NemId

Medarbejderne i Gribskov Kommune skal til de formål hvor dette er beregnet,

anvende medarbejder NemId, der er udsted til dem.

Personlig password, tilhørende en udsted medarbejder NemId, må på intet tidspunkt overdrages til kollegaer eller 3. person.

Ansvaret for rigtigheden af den enkelte medarbejders personlige oplysninger, påhviler til en hver tid den pågældende medarbejders nærmeste leder.

Medarbejder NemId udstedes af IT-organisationen efter bestilling.

Overskrift

Eksterne systemer

Formål med dette afsnit

Formålet med dette afsnit er at beskrive, hvorledes kommunen håndterer eksterne systemer.

Ansvarlig for område

Lederen af IT-drift

Afsnit sidst revideret - dato og navn

25.11.2015 - avlin

Beskrivelse

Ved beskrivelse af dette emne er der taget stilling til følgende problemstillinger: Baggrunden for dette er at der kan være omstændigheder der ved anvendelse af eksterne systemer i forhold til Gribskov Kommunes andre systemer, påkræver stillingtagen for så vidt angår sikkerheds-, og driftspørgsmål.

- Anvendelse af eksterne systemer (bilag 25).
- Anvendelse af tekniske løsninger til udveksling af data (bilag 26).
- Opsætning af systemadgang og adgangsgivning til eksterne systemer (bilag 27).

Overskrift

Datakommunikation

Formål med dette afsnit

At beskrive, hvilke vurderinger, der er foretage for at fastholde datasikkerheden under forsendelse, transmission og anden udveksling af information både internt og eksternt. Der skal være hurtig og sikker adgang til data, information og netværksressourcerne.

Formålet er at minimere konsekvenserne af manglende sikkerhed, som er følgende:

- Tyveri af informationer, hvor andre stjæler (kopierer) programmer, datafiler osv.
- Spredning af virus
- Bedragerier
- Dataindtrægning for at samle informationer, manipulere data eller ødelægge

data.
- Aflytning
- Personskade, når sikkerhedsalarmer og -systemer sættes ud af funktion.
- Blokering af store computersystemer. E-mail-systemet kan f.eks. blokeres ved, at man sender så store mængder e-mail, at modtageren ikke kan bearbejde dem alle, men får blokeret e-mail serveren. Dette kaldes normalt for "Denial of Service" (DOS).

Ansvarlig for område
Lederen af IT-Drift

Afsnit sidst revideret - dato og navn
25.11.2015 - avlin

Beskrivelse
I dette afsnit beskrives følgende:

1. Definationen af data
2. Netværk
3. Firewall
4. Internet og e-mail
5. Distancearbejdsplads
6. Kryptografi
7. Digital underskrift
8. Sociale medier (f.eks. facebook)

Datakommunikation

1. Datadefinition.
Data defineres som et hvert form for medie, hvorpå det er muligt at lagre information. Den mening, som en mængde data giver, kaldes for information. Datakommunikation er derfor synonym med informationsudveksling.

2. Netværk
Sikkerheden i Gribskov Kommunes netværk styrkes således, at alle transmitterende data og den underliggende infrastruktur er beskyttet. Personer, som forsøger at koble sig op til Kommunes netværk, bliver verificeret, så kun korrekte personer får adgang.
Følsomme oplysninger som overføres via Internettet sker med den såkaldte VPN teknologi.

VPN står for Virtual Private Network og kan skabe en krypteret tunnel via Internettet til PC-arbejdspladsen.

Datatilsynet anser trådløse netværk for en ekstern kommunikationsforbindelse. Der bør derfor ved anvendelse af trådløse netværk, træffes særlige foranstaltninger med henblik på at sikre sensitive data på samme niveau som på et lukket kablet netværk.

Der skal også sikres, at eventuelle uvedkommende, som skulle få adgang til det trådløse netværk, ikke derved kan aflytte kommunikationen og opsnappe brugeridentifikation og dertil hørende fortrolige adgangskoder, som anvendes i forbindelse med autoriserede brugers adgang til sensitive personoplysninger.

3. Firewall
Der skal være installeret en sikkerhedsforanstaltning (firewall), der regulerer trafik

til og fra internet.

Forsøg på uautoriseret brug og adgang til firewall'en logges. Firewall-installationen skal løbende vedligeholdes i takt med fremkomsten af stadig flere risici.

4. Internet og email
Internettet må benyttes af alle til tjenestelige formål.

Retningslinjer for håndtering af internet og email fremgår af bilag 22.

5. Ekstern opkobling
Anvendelsen af ekstern opkobling og bærbart udstyr, medfører en række yderligere risici, som kommunen ønsker at tage højde for. Det følger således af § 8 i bekendtgørelse om sikkerhedsforanstaltninger, at der ved arbejde fra fjernarbejdspladser og fra andre pc-arbejdspladser uden for den dataansvarliges lokaliteter, skal være øget fokus på sikkerheden. Henvisning til sikkerhed i forbindelse med IT-udstyr.

6. Kryptografi
Ved al datatransmission skal det overvejes alt afhængig af informationernes sensitivitet, om krypteringsfunktionalitet skal implementeres.

Der skal foretages kryptering baseret på en anerkendt algoritme.

Overskrift

Sikkerhed for datatransmission og netværk

Formål med dette afsnit

Formålet med dette afsnit er at beskrive de sikkerhedsforanstaltninger, der i Gribskov Kommune skal være gældende for datatransmission og netværk.

Ansvarlig for område

Lederen af IT-Drift

Afsnit sidst revideret - dato og navn

25.11.2015 - mptop

Beskrivelse

Det følger af § 14 i bekendtgørelse om sikkerhedsforanstaltninger, at der kun må etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.

Bestemmelsen gælder enhver form for telekommunikation i forbindelse med behandling af personoplysninger, f.eks. forsendelse af oplysninger med telefax eller ekstern e-post, etablering af terminaladgang ved opkaldsmodem, adgang til oplysninger via myndighedens hjemmeside og etablering af internetadgang fra arbejdspladser på myndighedens interne net. De særlige sikkerhedsforanstaltninger skal træffes efter myndighedens vurdering af sikkerhedsrisici i det konkrete tilfælde, herunder med hensyntagen til karakterne af de omhandlede oplysninger.

I dette afsnit beskrives det, hvilke sikkerhedsforanstaltninger der skal være gældende ved:
1. Datatransmission på egne fiber forbindelser (bilag 28).
2. Datatransmission på eksterne direkte forbindelser, f.eks. KMD (bilag 29).
3. Datatransmission via offentligt linier (bilag 30).
4. Sikkerhedsretningslinjer for netværk, generelt, og netværkkomponenter (bilag 31).
5. Anvendelse af trådløst netværk (bilag 32).
6. Der er i dette afsnit ikke noteret specielle tiltag omkring anvendelsen af ISDN, da disse i almindelighed ikke anvendes til primær datakommunikation.

Overskrift

Sikkerhed i.f.b.m IT Udstyr

Formål med dette afsnit

Med dette afsnit angives der at der konkret er taget stilling til de arbejdsmæssige og sikkerhedsmæssige aspekter i forhold til den fleksible anvendelse af IT der er present i Gribskov Kommune.

Ansvarlig for område

Lederen af IT-Drift

Afsnit sidst revideret - dato og navn

25.11.2015 - NSOLS

Beskrivelse

Gribskov Kommune udlevere en medarbejder pc som bruges på Gribskov Kommunes lokationer, samt mulighed for at anvende dette udstyr via eksternt opkobling.

Medarbejderen må ikke selv købe og installeres noget software eller hardware på medarbejder pc'en. Alt software der skal købes en licens til, skal installeres via IT.

Pc'ere udleveret af Gribskov kommune må kun anvendes til arbejdsmæssige formål. PC'en må ikke udlånes eller på anden måde benyttes af 3. part.

Sikkerhedshåndbog for Gribskov Kommune

Overskrift

Sikkerhedsforanstaltninger for anvendelse PC 'ere på netværk samt Bring Your Own Device (BYOD)

Formål med dette afsnit

Formålet med dette afsnit er at beskrive de retningslinjer som brugerne i Gribskov Kommune skal overholde i deres anvendelse af PC'er samt BYOD

Ansvarlig for område

Lederen af IT-Drift

Afsnit sidst revideret - dato og navn

Beskrivelse

Autorisation af brugere.

Virksomhedslederen har via inforådgiveren ansvaret for autorisation af medarbejderen.

I forbindelse med tildeling af autorisation eller ændringer i tildelte autorisationer anvendes følgende procedure:

1. Autorisationsbehovet kontrolleres og godkendes af info-rådgiverne eller leder.

2. Ændringer sker via henvendelse fra inforådgiver eller leder

3. Efter udstedelse af autorisation sørger systemansvarlig for, at der tildeles den pågældende en personlig adgangskode.

Den elektroniske adgangskode (password) skal følge Datatilsynets anbefalinger og dermed være på mindst 8 karakterer bestående af tal samt store og små bogstaver

Der må i adgangskoderne ikke anvendes en opbygning der kan henføres til den enkelte bruger eller dennes relationer. Der må heller ikke anvendes æ, ø, å.

I øvrigt skal autorisationskoderne udskiftes efter bestemmelserne i de respektive forskrifter, hvorved bemærkes, at der mindst hvert kvartal skal ske udskiftning af samtlige brugeres kodeord, for så vidt angår de systemer, hvor koden indtastes.

Har en medarbejder ikke længere behov for sin autorisation eller dele heraf, tager virksomhedsleder initiativ til inddragelse via inforådgiveren.

Den samme procedure iværksættes umiddelbart og senest inden 3 dage, når en medarbejder er fratrådt, subsidiært er blevet opsagt.

Observeres uregelmæssigheder vedrørende anvendelse af PC'erne, skal dette straks meddeles til Centerchefen eller et medlem af IT-sikkerhedsgruppen

Sikkerhedsregistrering og kontrol

For det IT-system, hvortil der er adgang via PC eller BYOD, indeholder bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (herefter bekendtgørelse om sikkerhedsforanstaltninger) særlige krav for anvendelsen, idet disse reglers krav til sikkerhedsforanstaltninger er gradueret ud fra bl.a. følsomheden af de oplysninger, systemet indeholder.

I henhold til § 18 i bekendtgørelse om sikkerhedsforanstaltninger skal der foretages en elektronisk registrering af alle uautoriserede adgangsforsøg, d.v.s. tilfælde hvor der indlæses/indtastes en ikke-gyldig autorisationskode. Der skal løbende følges op herpå.

Denne registrering skal ved den sikkerhedsansvarliges foranledning kontrolleres for hvert af systemerne mindst 1 gang i kvartalet.

Når den elektroniske sikkerhedsregistrering er kontrolleret, skal vurdering/erklæring efter omstændighederne eventuelt efter samtale med brugeren indføres i en rapport.

Uautoriseret brug af PC eller BYOD tilsluttet netværk

Hvis der foretages 5 uautoriserede adgangsforsøg inden for en bestemt periode, logges dette i de dertil værende logs.

Disse logs, der registrerer det uautoriserede adgangsforsøg, vil efterfølgene kunne kontrolleres for disse forsøg.

En brugers adgang lukkes automatisk, hvis der foretages 3 på hinanden følgende uautoriserede adgangsforsøg, og endvidere når der samlet indenfor 24 timer foretages mere end 15 uautoriserede adgangsforsøg.

Adgangen kan herefter kun åbnes efter forespørgsel til Helpdesk eller systemansvarlig.

Også i disse tilfælde skal der foretages en elektronisk registrering med henblik på opfølgning fra systemansvarliges side.

Registreringen skal ske i organisationens Helpdesk system.

Logning

Hvis bekendtgørelse om sikkerhedsforanstaltninger indeholder krav om elektronisk logning, er det den sikkerhedsansvarlige, der tager initiativ til kontrol af, at denne benyttelsesregistrering periodevis kontrolleres.

Umiddelbart efter at benyttelsesregistreringen er kontrolleret, foranstalter den sikkerhedsansvarlig en stikprøvevis undersøgelse af brugernes adfærd.

Denne kontrol foretages med henblik på en erklæring om, hvorvidt den registreredes anvendelse af systemet har været rimeligt begrundet i vedkommende brugers sagsbehandling.

Det forudsættes endvidere, at den enkelte bruger inddrages i undersøgelsen.

I henhold til bekendtgørelse om sikkerhedsforanstaltninger skal der foretages maskinel registrering af alle PC og terminalforespørgsler dvs. benyttelseskontrol.

For de IT-systemer, der indeholder mere følsomme personoplysninger, skal der foretages en differentieret elektronisk logning, dvs. registrering af alle forespørgsler og/eller opdateringer og sletninger af bestemte mere følsomme typer af oplysninger (retslige/sociale/helbredsmæssige) i systemet, hvilket i praksis betyder, at der foretages en fuldstændig logning af bestemte skærmbilleder for de systemer, hvor dette er gældende.

Kontrol af den differentierede logning, der skal foretages mindst 1 gang i kvartalet, på foranledning af data-sikkerhedsansvarlig.

Loggen opbevares i 6 måneder, hvorefter den skal slettes.

Det skal bemærkes, at der intet lovmæssigt krav er til, at loggen skal udskrives.

Opbevaring på et elektronisk medie eller lagring i selve det elektroniske sikkerhedssystem er fyldestgørende.

Procedure og behandling af logningsmateriale fra sikkerhedssystemet

Efter gennemgang af alt logningsmateriale fra sikkerhedssystemerne udfærdiges en rapport/logbog.

Indhold:

1. Intet at bemærke
2. Fejlbetjening
3. Uautoriseret anvendelse
4. Grundlag for ændring af autorisation
5. Udtræk i overensstemmelse med relevant sagsbehandling
6. Konstateret misbrug/ikke-tjenstlig benyttelse

I tilfælde af konstateret misbrug rapporteres straks til den sikkerhedsansvarlige.

Den sikkerhedsansvarlige indkalder relevante medarbejdere til møder i det omfang, det skønnes nødvendigt.

Tiltag: Check af sikkerhedsrutiner
Frekvens: Jvf. sikkerheds årshjul (årligt)
Ansvar: Den overordnede sikkerhedsansvarlige
Kommunikation: Resultat meldes ud i organisationen og eventuelle opfølgningspunkter afrapporteres efterhånden som de afklares/løses.
Beskrivelse af tiltag - der oprettes 1 afsnit som dette for hvert tiltag.

Bilag
Overskrift for og link til bilag - der oprettes 1 afsnit som dette for hvert bilag.

Bilagets overskrift

Sikkerhedsforeskrifter, Gribskov Kommune

Formål med dette bilag
Beskrivelse af hvilke regler der er gældende for opbygning af password

Ansvarlig for bilagets indhold
Leder af IT-drift

Bilag sidst revideret - dato og navn
25.11.2015 - aviln

Beskrivelse
Virksomhedslederen har ansvar for autorisationer af medarbejderne til arbejdsrelevante systemer.

Inforådgiver har ansvar for at undersøge relevansen - evt. i samarbejde med virksomhedslederen - af, om en bruger skal have en autorisation til et system og for at bestille autorisationen hos den systemansvarlige.

Systemansvarlig har ansvar for at autorisere brugere efter bestilling fra inforådgiver, og at brugeren tildeles personlig adgangskode efter reglerne for det pågældende system. Systemansvarlig er ansvarlig for løbende at kontrollere, at autorisationsområderne er i overensstemmelse med den enkeltes autorisation i forhold til bestillinger fra inforådgiver samt at gøre virksomhedsleder og data-sikkerhedsansvarlig opmærksom på uoverensstemmelser og eventuelt at inddrage en autorisation.

Den sikkerhedsansvarlige skal straks underrettes ved misbrug og er koordinerende på dette område med hensyn til kontrol for eksempel via logningsmøder.

IT-organisationen er ansvarlig for elektronisk at registrere alle uautoriserede adgangsforsøg. Kontrolleres minimum 1 gang hvert halve år.

Den sikkerhedsansvarlige er ansvarlig for at bestille kontrol af at benyttelsesregistrering, hvis Persondatalovens cirkulærer og vejledninger indeholder krav om elektronisk logning.

Den sikkerhedsansvarlige er ansvarlig for at bestille kontrol - hvert halve år - af den differentierede elektroniske logning (registrering af alle forespørgsler og/eller opdateringer og sletninger af bestemte mere følsomme typer af oplysninger - retslige/sociale/helbredsmæssige - i systemet, hvilket i praksis betyder, at der foretages en fuldstændig logning af bestemte skærmbilleder).

Sikkerhedsforanstaltninger for Gribskov Kommune.

Stationære og Bærbare pc'er.

I dette afsnit er der forholdsregler, som medarbejdere skal gøre sig bekendt med, samt efterleve i deres anvendelse af pc arbejdspladser.

Sikring mod tyveri

Medarbejdere skal sørge for, at de forsvarligt sikrer deres pc'er.

Dette gøres ved, at bærbare pc'er ved transport opbevares i den taske, som er leveret sammen med udstyret.

Opbevaring af IT udstyr i egen bil, skal ske ved at udstyret placeres i et låst rum, hvor til det ikke er muligt at foretage en visuel genkendelse af udstyret, eller den taske som udstyret er placeret i.

Medarbejdere skal kontrollere, at deres IT udstyr er tydeligt mærket med tilhørsforhold, Gribskov Kommune.

Medarbejdere skal sikre, at deres bærbare arbejdsstationer ikke efterlades synligt i lokalet, men er låst inde, hvis de forbliver på arbejdspladsen.

Sikring mod misbrug

Medarbejderen skal låse sin arbejdspc (ctrl + alt + delete), når vedkommende forlader sin arbejdsplads.

Arbejdsrelateret data **skal** gemmes i sagsbehandlingssystemer og om nødvendigt midlertidigt på medarbejdernes personlige netværksdrev eller på afdelingens netværksdrev.

Sikring mod virus/hacking

På alle pc'er skal der være installeret et antivirus program. Medarbejderen skal kontrollere, at dette er tilfældet, og hvis ikke, kontakte IT organisationen for at få dette etableret.

Alle pc'er bliver løbende opdateret med sikkerhedsopdateringer.

Medarbejderne må under ingen omstændigheder påvirke sådanne opdateringer på en sådan måde, at opdateringer ikke bliver udført.

Vejledning i opbygning af password.

Formål med dette afsnit

Afsnittet her beskriver de forhold der er omkring datasikkerhed, driftssikkerhed og lovlighed, når ny software og dermed nye måder at behandle informationer på bringes til veje - enten via indkøb eller ved udvikling af software i kommunen.

Ansvarlig for område

Chefen for IT-organisationen

Afsnit sidst revideret - dato og navn

25.11.2015 - aviln

Beskrivelse

Opdeling

Situationen, hvor software udvikles internt i Gribskov Kommunes organisation adskiller sig fra situationen, hvor software indkøbes, idet der ikke i samme grad sker overdragelse af ansvar i processen. Hvor intern udvikling derfor må fokusere direkte på relevant sikkerhed og driftsstabilitet i programmerne, må indkøb ofte overlade i det mindste en del af dette ansvar til en leverandør, hvorfor kommunens processer i højere grad må fokusere på aftaleforholdet med denne leverandør.

Intern udvikling

Det skal sikres, at ny-udvikling og videreudvikling af software ikke bringer kommunens driftsstabilitet i fare, samt at informationssikkerheden overholdes. For bedst at gøre dette skal følgende tiltag gøres.

Ved inddragelse af ekstern bistand i denne sammenhæng henvises til retningslinier for ekstern bistand (bilag 33).

Sikkerhed for drift under udvikling

Det skal sikres, at udviklingsmiljø og produktionsmiljø er adskilte, således at fejl og mangler i et testforløb ikke kan påvirke den daglige drift.

Test af produkt i lukket, men sammenligneligt miljø

Miljø for udvikling og test skal så vidt muligt simulere opsætningen for de rigtige systemer mhp. at sikre mod uforudsete driftsforstyrrelser efter ibrugtagning.

Sikring af, at alle aspekter checkes

Sikring af, at alle aspekter checkes ved bred inddragelse i organisationen ifm. udarbejdelse af testkatalog.
Review af testkataloget skal sikre, at alle grænseflader mht. påvirkede systemer, data-lagre, arbejdsgange og kommunikationsrutiner tages i betragtning.

Indkøb af software

Vi overholder de til en hver tid de gældende regler for udbud og indkøb.

Leverandørs soliditet

Der skal foretages en undersøgelse eller i det mindste overvejelse af leverandørens soliditet mhp. at minimere risiko ift. fortsat support etc. Dette gælder både den direkte leverandør og den oprindelige producent af softwaren. Omfanget af en sådan vurdering skal stå mål med investering, betydning og

risiko i det hele taget.

Leverandørs erfaring med sammenlignelige kunder
Der skal foretages en undersøgelse af leverandørs erfaring med sammenlignelige kunder for så vidt muligt at sikre mod uforudsete driftsforstyrrelser efter ibrugtagning. Ved indkøb af of-the-shelf software, som ligeledes kan købes gennem andre leverandører, kan dette trin springes over.

Forventninger til ydelse
Der skal ske en beskrivelse af krav til system, såsom svartider, kapacitet og andre relevante aspekter ift. kommunens konkrete tekniske set-up og forventet belastning. Denne beskrivelse og overvejelse skal afvejes i forhold til investering, risiko, vigtighed for driften og økonomi.

Sanktioner ved mangler
Sanktioner ved manglende opfyldelse fra leverandørs side skal beskrives - især mhp. at sikre eventuel assistance til nødløsninger, hvor fejl opstår. Ved indkøb af of-the-shelf software, som ligeledes kan købes gennem andre leverandører, kan dette trin springes over.

Overskrift

Foranstaltninger ved andet informationsteknologisk udstyr

Formål med dette afsnit

Det skal sikres, at andet udstyr end almindelige PC'er udgør eller genererer nogen unødig risiko.

Ansvarlig for område

Lederen af IT-Drift

Afsnit sidst revideret - dato og navn

25.11.2015 - aviln

Beskrivelse

Fax

Der skal være klare retningslinier for afsendelse og modtagelse af sensitive papirer fra fax.

Mobiltelefon

Der skal være klare retningslinier for brug af mobiltelefoner i forbindelse med sensitive oplysninger.

Videoovervågning

Videoovervågning igangsætte kun efter anmodning fra risikorådgiver.

Nye typer udstyr

Der skal være defineret hvordan nye typer udstyr skal vurderes mhp. sikkerhed,

når de tages i brug af Gribskov Kommune.

Ovennævnte er udspecificeret i bilag 34.

Overskrift

Fysisk sikkerhed på farten

Formål med dette afsnit

Afsnittet beskriver overordnede retningslinier for de basale fysiske og omgivelsesmæssige krav omkring den fysiske sikkerhed når en medarbejder er på farten i den offentlige steder.

Ansvarlig for område

Lederen af IT-Drift

Afsnit sidst revideret - dato og navn

25.11.2015 - aviln

Beskrivelse

IT-sikkerheden er også vigtig, når man arbejder hjemme eller er på farten, og at der som udgangspunkt gælder de samme normer for adfærd i forbindelse med hjemmearbejde eller arbejde på farten som på arbejdspladsen.
Din adgang til IT-systemerne må kun bruges af dig.
Dit kodeord er personligt – Pas godt på det.
Der en risiko for sikkerhedsbrud ved at organisationens medarbejdere og ledere mod deres vilje videregiver information, enten mundtligt eller skriftligt (ved at uvedkommende læser med på papir eller skærm). Det samme gælder for arbejde på bærbare computere eller mobile enheder.

Mobilt udstyr:
Dit mobile udstyr kan indeholde følsomme oplysninger. Du skal holde opsyn med dit udstyr på farten.
Mobilt udstyr er alt, hvad du medbringer, der indeholder information. Det kan være mange ting, f.eks.:

- Mobil tlf.
- Ringbind og papir
- Mobile enheder
- Bærbar
- USB-nøgle
- CD-ROM

Hjemmearbejde:
Hjemmearbejde foregår ofte ved hjælp af en medarbejder-pc, der tilhører Gribskov Kommune. Medarbejder pc'en er konfigureret af Gribskov Kommunes IT, så dele af de ovennævnte risici imødegås.
Bærbare computere og mobil telefoner bliver ofte stjålet, og derfor bør den mobile

udstyr sikres forsvarligt både fysisk samt med krypteret kodeord.

Privat udstyr:
Hold dit private udstyr adskilt fra dine arbejdsopgaver.
Hvis hjemmearbejde foregår på en privat computer, er der risiko for, at den ikke har samme sikkerhedsniveau som organisationens interne computere. Det kan udgøre en alvorlig sikkerhedsrisiko at lagre følsom information på privat udstyr. Og der kan der opstå licensmæssige problemer, hvis der installeres privat software på arbejdscomputere.
Se bilag 35 vedrørende Medarbejderes forpligtelse ved distance arbejde.

Overskrift

Registrering af aktiver

Formål med dette afsnit

Formålet beskrives her

Ansvarlig for område

Lederen af IT-Drift

Afsnit sidst revideret - dato og navn

25.11.2015 - holse

Beskrivelse

Der skal være en opgørelse over alle systemmæssige aktiver.

Der skal også være taget stilling til forsikring af vigtige aktiver. Gribskov Kommune er i høj grad selvforsikret eller har valgt forsikringer med høj selvrisiko. Det betyder bl.a. at fysiske aktiver alene er forsikret mod skader opstået ved brand, storm samt oversvømmelser ved skybrud eller lignende. Der er for disse hændelser en selvrisiko på 100.000 kr. (2012 niveau).

Aktiver i form af hardware skal være tyverimærket.

Se i dette bilag 37.

Overskrift

Dokumentation

Formål med dette afsnit

Sikkerhedsniveauet skal være dokumenteret for at være operationelt

Ansvarlig for område

IT-Sikkerhedsgruppen

Afsnit sidst revideret - dato og navn

25.11.2015 - aviln

Beskrivelse

Som et gennemgående tema i kommunens IT-sikkerhedshåndbog og bilag, skal det valgte IT-sikkerhedsniveau - samt den daglige håndtering af IT-sikkerheden - være dokumenteret.

Dokumentation af systemer og forretningsgange skal sikre, at en almindelig IT-kyndig kan skabe sig tilstrækkelig indsigt i konstruktioner og procedure til at kunne videreføre systemerne. Endvidere skal dokumentationen sikre en tilfredsstillende bevisførelse, hvis it- anvendelsen - og dermed IT-sikkerheden - skulle give anledning til uenighed.

For alle væsentlige systemer og IT-relaterede forretningsgange skal der foretages en vurdering af behovet for dokumentation af virkemåde, procedure mv. Dette gælder både driftsopgaver, sikkerhedsadministration og teknisk opsætning.

Overskrift

Medarbejdersikkerhed (organisatoriske og medarbejdermæssige forhold)

Formål med dette afsnit

Alle medarbejder skal være opmærksomme på deres særlige ansvar i forbindelse med anvendelse af kommunens IT-aktiver og IT-baserede infrastruktur.

Ansvarlig for område

IT-Sikkerhedsgruppen

Afsnit sidst revideret - dato og navn

25.11.2015 - aviln

Beskrivelse

Alle medarbejdere skal have kendskab til og arbejde i overensstemmelse med kommunens IT-sikkerhedspolitik og relaterede regler. Endvidere er tiltag, som skal medvirke til, at alle medarbejdere har en sikkerhedsorienteret kultur og bevidst holdning til begrebet IT-sikkerhed, hvor der lægges vægt på reel sikkerhed frem for formel sikkerhed. Dette sker bl.a. ved informationsmateriale ifm ansættelse

Ledelsens/virksomhedens ansvar

Kommunens ledelse har ansvaret for, at alle IT-brugere har kendskab til - og arbejder efter IT-sikkerhedshåndbogen samt relevante bilag. Det betyder blandt andet, at alle IT-brugere skal orienteres om deres ansvar i forbindelse med IT-sikkerheden, forinden der gives adgang til systemer og data. Relevante retningslinier skal være formidlet til alle IT-brugere og ledelsen skal sikre et betryggende IT-sikkerhedsniveau hos alle brugere ved selv at gå forest når det gælder en betryggende og tilstrækkelig IT-sikkerhed. Roller i forhold til sikkerheden ses her: bilag 4.

Uddannelse

Alle medarbejdere, der arbejder med kommunens IT-udstyr, skal modtage den nødvendige instruktion i kommunens IT-sikkerhedsregler og forretningsgange. Endvidere skal der løbende ske efteruddannelse således, at medarbejderens viden og IT-anvendelsen og IT-sikkerheden til stadighed er ajourført.

Brud på IT-sikkerheden

Ansvaret for at efterleve sikkerheden omkring IT-anvendelsen i Gribskov

Kommune, er placeret hos hver enkelt medarbejder. Det skal derfor fremhæves, at overtrædelse af IT-sikkerheden efter omstændighederne kan medføre sanktioner. Hvis en medarbejder opdager trusler i mod kommunens IT-driftsafvikling eller er bekendt med overtrædelse af IT-sikkerhedsreglerne, skal dette meddeles nærmeste centerchef eller et medlem af IT-sikkerhedgruppen hurtigst muligt . Se også afsnit om misbrug: bilag 36.

Ansættelsens ophør
Når en IT-bruger fratræder sin stilling, skal der være etableres konsekvente forretningsgange, der både sikrer betryggende sletning af autorisationer samt at kommunens IT-aktiver returneres.

Eksterne medarbejdere
Hvis eksterne medarbejdere fra f. eks. servicefirmaer eller samarbejdskommuner i perioder er udstationeret i organisationen, eller der er længerevarende aftale om samarbejde, som giver adgang til IT-informationer og systemer, skal medarbejderen underskrive en "Tro og love erklæring" i henhold til Straffelovens § 152. Der skal i alle tilfælde være beskrevet faste procedurer for, hvordan såvel fysisk som logisk adgang til systemerne sker for eksterne medarbejdere herunder rutiner for oprettelse og sletning af adgang.

Inforådgiver
Alle afdelinger har tilknyttet inforådgiver, som assisterer med udførelse af de medarbejderrelaterede IT-opgaver - herunder også assistance til nærmeste centerchef med de sikkerhedsmæssige aspekter
Inforådgiveren er hjælper med følgende opgaver:

- Adgange til IT-systemer, telefoni, adgangskort mm.
- Bestilling af IT-udstyr og telefon
- Undervisning af og information til nye medarbejdere
- Nye systemer og ændringer i nuværende systemer
- Rådgivning og vejledning
- Kendskab til generel anvendelse af systemer i ansvarsområdet

Bilag
Medarbejdersikkerhed/personlige forhold - bilag 6 .

Overskrift

Misbrug ift. sikkerhedsbestemmelserne

Formål med dette afsnit

Kommunen ønsker at kommunikere klart til alle brugere af systemet, at overtrædelse af sikkerhedsbestemmelser har en konsekvens.

Ansvarlig for område

IT-Sikkerhedsgruppen

Afsnit sidst revideret - dato og navn

25.11.2015 - aviln

Beskrivelse

Konstatering af overtrædelser

Overtrædelse af sikkerhedsbestemmelserne kan i princippet ske bevidst eller ubevidst. Med denne sikkerhedshåndbog og de deraf følgende tiltag sikres det at den enkelte medarbejder er sit ansvar bevidst i de situationer, hun/han måtte komme i.

Der overvåges på alle relevante områder iht. tiltag beskrevet andetsteds i denne håndbog, at sikkerheden overholdes på alle 3 relevante områder

- Driftsikkerheden
- Informationssikkerheden/fortrolighed - internt og eksternt
- Lovligheden i IT-anvendelse

Skulle der alligevel ske overtrædelser af bestemmelserne som generer en risiko på et eller flere af områderne, er den, som opdager overtrædelsen forpligtet til at informere områdechefen eller IT-sikkerhedsgruppen om overtrædelsen så hurtigt som muligt.

Sanktioner

Sanktioner besluttes i fællesskab i organisationen med inddragelse af de relevante parter ift. det område overtrædelsen er sket på, samt hvem der er blevet ramt og hvor overtrædelsen har medført en risiko. Sanktioner skal sættes i relevant perspektiv til følgende:

- Overtrædelsens forsætlighed
- Gentagelser
- De konsekvenser, den har medført
- Den generelle risiko, der er blevet påført organisationen
- Forvaltningsloven

Overskrift

Eksterne samarbejdspartnere

Formål med dette afsnit

Formålet med dette afsnit er at beskrive, hvornår der skal indgås en kontrakt med en ekstern samarbejdspartner. Formålet er endvidere at give et overblik over, hvilke forhold, der skal overvejes i forbindelse med, at der skal indgås en kontrakt.

Ansvarlig for område

IT-Sikkerhedsgruppen

Afsnit sidst revideret - dato og navn

25.11.2015 - aviln

Beskrivelse

Eksterne samarbejdspartnere

Det kan udgøre en risiko at give en samarbejdspartners medarbejdere adgang til interne faciliteter og informationer, blandt andet fordi samarbejdspartnerens styring af sikkerhed kan være utilstrækkelig. Hvor der er et forretningsmæssigt behov for data- og/eller systemadgang, skal der foretages en risikovurdering.

Hvis risikovurderingen viser, at der er en væsentlig risiko forbundet med en samarbejdspartners adgang til virksomhedens informationsbehandlingsfaciliteter eller andre former for samarbejde, skal samarbejdet baseres på en formel

kontrakt. Begge parter skal være enige i de sikkerhedskonditoner, der er knyttet til samarbejdet. Kontrakten skal færdigbehandles og underskrives, før dens tekniske og kontrolmæssige indhold implementeres.

Ved samarbejde med andre parter, der har adgang til virksomhedens informationsaktiver, skal der gennemføres en risikovurdering, og relevante sikringsforanstaltninger skal identificeres og implementeres.

Risikovurderingen skal omfatte:

- de informationsbehandlingsfaciliteter samarbejdspartneren skal have adgang til
- hvilken form for adgang samarbejdspartneren skal have (fysisk adgang, logisk adgang, om adgangen skal være via internt net eller via opkobling)
- den forretningsmæssige værdi af de involverede informationsaktiver
- beskyttelsesforanstaltninger for informationsaktiver, der ikke er omfattet af samarbejdet
- samarbejdspartnerens personale
- autorisations- og verifikationsprocedurer
- samarbejdspartnerens informationslagrings-, behandlings- og kommunikationsudstyr og de hertil knyttede sikringsforanstaltninger
- konsekvenserne af manglende tilgængelighed og ukorrekte informationer
- procedurer for håndtering af sikkerhedsrelaterede hændelser
- særlig lovgivning, samarbejdspartneren skal tage hensyn til, og andre kontraktforhold, virksomheden og/eller samarbejdspartneren skal tage hensyn til
- hvorledes samarbejdet vil påvirke øvrige interesser.

Samarbejdspartneren må ikke få adgang til virksomhedens informationer før risikovurderingen er gennemført, de relevante sikringsforanstaltninger er implementeret, og der, hvor det er påkrævet, er indgået en formel samarbejdsaftale.

Det skal sikres, at samarbejdspartneren er klar over sine forpligtelser og sit ansvar i forbindelse med den indgåede aftale.

Ved indgåelse af en samarbejdsaftale, skal følgende punkter vurderes:

- virksomhedens informationssikkerhedsmålsætning
- de aftalte sikringsforanstaltninger som eksempelvis:
  1. procedurer til beskyttelse af virksomhedens informationsaktiver
  2. eventuelle fysiske beskyttelsesforanstaltninger
  3. beskyttelse mod skadevoldende programmer
  4. procedurer for konstatering af eventuelle sikkerhedsbrud
  5. procedurer for returnering eller destruktion af information ved aftalens udløb eller på andet aftalt tidspunkt
  6. procedurer til beskyttelse af integritet, tilgængelighed og autenticitet
  7. restriktioner vedrørende kopiering og videregivelse
- brugeruddannelse
- brugerbevidstgørelse
- mulighed for eventuel udveksling af personale
- ansvaret for installation og vedligehold af informationsbehandlingsudstyr og programmel
- rapporteringsomfang, -struktur og -format
- procedurer for ændringsstyring
- adgangskontrolprocedurer
  1. den forretningsmæssige begrundelse for at give samarbejdspartneren adgang
  2. tilladte adgangs- og identifikationsmetoder
  3. autorisationsprocedure for brugeradgang og tildeling af rettigheder og

præcisering af, at adgangstildeling og - rettigheder skal være strengt arbejdsbetinget
4. krav til lister over brugeradgang og -beføjelser
5. præcisering af at enhver uautoriseret adgang er forbudt
6. procedure for spærring af adgangsrettigheder

- procedurer for rapportering og efterforskning af sikkerhedsbrud og -hændelser samt overtrædelse af samarbejdsaftalen
- beskrivelse af det informationsbehandlingsudstyr, de systemer og de informationer, der er omfattet af aftalen
- det aftalte kvalitetsmål for serviceydelsen
- beskrivelse af de aftalte servicemål, deres overvågning og afrapportering
- retten til at overvåge og afbryde den aftale serviceydelse
- retten til revision af kontraktens overholdelse, evt. ved brug af ekstern revisor
- eskaleringsprocedure ved problemhåndtering
- beredskabsplaner, herunder krav til maksimal retableringstid
- de respektive parters ansvarsforhold i relation til aftalen
- ansvarlighed i forhold til lovbestemmelser, eksempelvis persondataloven.
- forhold omkring ophavsrettigheder og licenser
- aftaleforhold i forbindelse med samarbejdspartnerens eventuelle underleverandører
- betingelserne for genforhandling/afslutning af samarbejdsaftalen
  1. ved brud på aftalen
  2. ved ændringer til sikkerhedskravene
  3. dokumentationen af aftalens indhold og omfang, licenser, aftaler og rettigheder skal til stadighed holdes ajour.

Hvis samarbejdsaftalen vedrører drifts- og vedligeholdelsesydelser hos en driftsleverandør, så skal aftalen beskrive, hvorledes leverandøren vil sikre det aftalte sikkerhedsniveau ved ændringer i risikobilledet. Endvidere skal alle forhold i forbindelse med en eventuel afbrydelse af samarbejdet være beskrevet, specielt hvis afbrydelsen skyldes leverandørens manglende evne til at levere den aftalte ydelse.

Overskrift

Ikrafttræden

Formål med dette afsnit

Afsnittet beskriver, hvornår sikkerhedshåndbogen gælder.

Ansvarlig for område

IT-Sikkerhedsgruppen

Afsnit sidst revideret

25.11.2015 - avlin

Beskrivelse

IT-sikkerhedshåndbogen gennemgås mindst én gang om året med henblik på at sikre, at de interne bestemmelser er fyldestgørende og afspejler de faktiske forhold i kommunen, jf. bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.

Underdokumenter:

<FONT face=Verdana size=1>
</FONT>