Greve Kommune

It-sikkerhedspolitik

Center for Byråd & Økonomi 2013

Indhold

1. Introduktion til it-sikkerhedspolitikken

Baggrund

Anvendelsen af it i Greve Kommune er med tiden blevet mere kompleks. Kommunen anvender på flere områder og i større omfang med fordel it for at leve op til de krav som borgere, samfundet og lovgivningen stiller til en effektiv administration og til en hurtig og korrekt service.

Kommunen vil som et naturligt led i den generelle udbygning af den tekniske it-anvendelse og med udgangspunkt i ISO 27001 samle og præcisere eksisterende it-sikkerhedsmæssige retningslinjer, som er gældende for it-brugere i hele Greve Kommune.

Formål

Formålet med it-sikkerhedspolitikken er at sikre kommunens borgere, virksomheder og medarbejdere adgang til en tilgængelig, pålidelig og fortrolig kommunal service. Det opnås ved:

- At Greve Kommune i overensstemmelse med god offentlig forvaltningsskik sikrer data og informationers fortrolighed, pålidelighed, integritet og tilgængelighed. Derved opnås Greve Kommunes primære målsætning; at servicere kommunens borgere, virksomheder og medarbejdere effektivt og på den bedst mulige måde.

- At it-sikkerhedsniveauet i Greve Kommune til hver en tid er i overensstemmelse med gældende lovgivning, kontraktuelle krav og god it-skik. Kommunen har over for personer og virksomheder i henhold til lovgivningen et særligt ansvar for at beskytte oplysninger om personer mod uautoriseret anvendelse og mod fejl i oplysningerne.

- At Greve Kommunes it-sikkerhed er tilpasset de informationer, som skal beskyttes, set i forhold til de trusler, som kan forårsage tab af fortrolighed, pålidelighed, integritet og tilgængelighed. It-sikkerheden fastholdes igennem såvel løbende kontroller som uddannelse og information på tværs af organisationen, hvor det måtte være påkrævet.

- At Greve Kommune tilsigter, at anvendelsen af og funktionaliteten i kommunens it-systemer ikke forringes som følge af it-sikkerhedsniveauet. It-sikkerheden indgår i stedet som en integreret og ikke begrænsende del af arbejdsprocesserne i kommunen, så it-sikkerhedsrelaterede procedurer og kontroller er en normal del af arbejdsprocesserne.

- At Greve Kommunes it-sikkerhed understøtter kommunens strategiplan samt de generelle værdier kommunen har som arbejdsplads og servicefunktion overfor kommunens borgere og virksomheder.

- At Greve Kommune fastholder it-sikkerhedsniveauet gennem krav til adfærd samt målretter formidling af viden omkring it-sikkerhed til de medarbejdere og eksterne parter, der måtte have kontakt med de kommunale it-ressourcer.

Gyldighed og omfang

It-sikkerhedspolitikken bliver løbende opdateret, og bliver gennemgået en gang årligt. It-sikkerhedsudvalget vurderer, hvornår der er behov for politisk behandling og underretter MED-systemet, hvis der ændres i personalerelaterede forhold. Redaktionelle ændringer kan uden videre foretages.

Alle brugere, samarbejdspartnere, institutioner o.l. samt leverandører med fysisk eller logisk adgang til kommunens systemer skal være bekendt med it-sikkerhedspolitikken og er forpligtet til at overholde reglerne.

2. Organisation og ansvar

Generelt

Rollerne og det medfølgende ansvar, som nævnes i it-sikkerhedspolitikken, er alene beskrevet i forhold til it-sikkerheden i Greve Kommune. Det betyder at yderligere ansvar tildelt disse roller, er beskrevet andetsteds.

Byrådet og Direktionen

Byrådet har det overordnede ansvar for etablering og vedligeholdelse af en it-sikkerhed, der er tilpasset Greve Kommunes behov og opfylder kravene i lovgivningen og god forvaltningsskik.

Byrådet har delegeret ansvaret for den daglige ledelse og kontrol af it-sikkerheden til kommunaldirektøren. Direktøren skal i samarbejde med It-sikkerhedsudvalget og Center for Byråd & Økonomi præcisere it-sikkerhedsniveauet, og sikre overholdelse af it-sikkerhedsreglerne i kommunen. Direktøren for det sociale område har det overordnede ansvar for overholdelsen af persondataloven og skal overordnet sikre kommunens efterlevelse af Datatilsynets regler og krav.

It-sikkerhedsudvalget

It-sikkerhedsudvalget består af centerchefen for Center for Byråd & Økonomi, It-chefen, Risikokoordinatoren, en medarbejder fra Center for Byråd & Økonomi med kendskab til it-sikkerheden samt en jurist med kendskab til persondataloven og god sagsbehandlingsskik.

It-sikkerhedsudvalget har ansvaret for at udarbejde og opdatere it-sikkerhedspolitikken og for at bidrage til, at it-sikkerhedspolitikken implementeres effektivt i Greve Kommune. It-sikkerhedsudvalget rapporterer, når det er påkrævet, om det faktiske it-sikkerhedsniveau i kommunen til Kommunaldirektøren og Byrådet.

Center for Byråd & Økonomi vurderer de sikkerhedsmæssige og koordineringsmæssige aspekter af it-investeringer, ændringer i den anvendte teknologi eller andre forhold, som har indflydelse på it-sikkerheden i kommunen. En medarbejder etablerer og vedligeholder kontroller og procedurer til at overvåge, hvor effektivt it-sikkerheden er implementeret i kommunen.

It-chefen

It-chefen har ansvaret for:

- den tekniske it-sikkerhed, herunder netværkssikkerhed, virusbeskyttelse, driftsstabilitet mv.
- den administrative it-sikkerhed baseret på blandt andet datas klassifikation
- at netværket er korrekt dokumenteret, og at driften og udviklingen af det enkelte netværk sker i overensstemmelse med de vedtagne procedurer, sikkerhedsforskrifter og kontroller. It-chefen er desuden ansvarlig for at rapportere fejl og afvigelser til It-sikkerhedsudvalget.

Centerchefer

Centercheferne er ansvarlige for, at it-sikkerheden overholdes i deres centre og at:

- opgaverne i centre + institutioner udføres efter regler og instrukser i it-sikkerhedspolitikken og øvrige retningslinjer
- medvirke til dokumentation af behovet for it-sikkerhed inden for egen organisation
- sikre medarbejdernes kendskab til gældende regler og instrukser samt
- føre tilsyn med at regler og instrukser overholdes
- samarbejde med It-sikkerhedsudvalget og It-chefen
- Systemejerskabet løftes for de systemer, som centerchefen er systemejer for.

Risikokoordinator

Risikokoordinatoren har overordnet ansvaret for fysisk sikkerhed på rådhuset og tv-overvågning i kommunen.

Systemejere

Centercheferne har systemejerskabet for it-systemerne i deres center og derved for dokumentation og vedligeholdelse. Systemejerens ansvar er beskrevet i "Vejledning i systemejerskab i Greve Kommune", og de konkrete opgaver kan delegeres af centerchefen til en medarbejder, der udpeges som systemansvarlig.

Brugerinstruktører

Brugerinstruktøren (BI) er relationen mellem BI´ens center og Center for Byråd & Økonomi. Der er udpeget en eller flere brugerinstruktører for hvert center.

En BI er udpeget af sit center i samarbejde med It, og er autoriseret til at varetage sit centers brugeradministration på det administrative it-netværk. Det indbefatter at sørge for, at nye medarbejdere i centeret bliver oprettet på Greve Kommunes it-netværk med de rettigheder, som er nødvendige for deres jobfunktion. Ligeledes gælder, at BI´en skal nedlægge medarbejdernes it-profiler, hvis de fratræder, eller ændre it-profilen, hvis der sker ændringer i medarbejdernes jobfunktioner.

It-vejledere

It-vejlederen er relationen mellem it-vejlederens skole og Center for Byråd & Økonomi. Der er udpeget en eller flere it-vejledere for hver skole.

It-vejlederen er ansvarlig for, at nye medarbejdere og elever bliver oprettet på skolenetværket med de rettigheder, som er nødvendige for deres jobfunktion. Ligeledes skal it-vejlederen nedlægge medarbejdernes it-profiler, hvis de fratræder, eller ændre it-profilen, hvis der sker ændringer i medarbejdernes jobfunktioner.

3. Medarbejdersikkerhed

Generelt

Medarbejdersikkerheden sikrer, at Greve Kommunes it-ressourcer ikke udsættes for risici i forbindelse med brugen af disse, ligesom medarbejdere sikrer sig, at deres færden logisk (på pc-arbejdspladserne) såvel som fysisk (fysiske behandling af it-udstyret) er i overensstemmelse med retningslinjerne, som er udstukket af Center for Byråd & Økonomi.

Alle retningslinjer og politikker på it-sikkerhedsområdet er offentliggjort under Fælles viden og It på Mit Greve (intranettet).

Før ansættelse

Medarbejdere i Greve Kommune bliver før ansættelse oprettet som bruger på Greve Kommunes it-ressourcer på foranledning af en brugerinstruktør fra det center, medarbejderen skal starte i eller fra it-vejlederen på skolen. Centeret har herefter til ansvar at udlevere pixi-udgaven af Greve Kommunes it-sikkerhedspolitik samt informere den nye medarbejder om hvor den fulde it-sikkerhedspolitik kan findes, så vedkommende fra samarbejdets start er bekendt med denne.

Under ansættelse

Bevidst såvel som ubevidst overtrædelse af it-sikkerhedsbestemmelserne kan medføre, at kommunens brugere, samarbejdspartnere, borgere mv. oplever ustabilitet, uregelmæssigheder og uhensigtsmæssigheder i indtastning, anvendelse eller bearbejdning af data i et eller flere it-systemer, hvilket er uacceptabelt.

Overtrædelser af it-sikkerhedspolitikken håndteres af den daglige leder, for eksempel i form af kontakt til de involverede medarbejdere med henblik på en nærmere afdækning af hændelsesforløb, baggrund og karakteren af overtrædelsen.

I alvorlige eller generelle tilfælde skal sagen i direktionen. Overtrædelse af it-sikkerhedspolitikken kan få ansættelsesmæssige konsekvenser.

Som bruger på Greve Kommunes it-netværk skal man være specielt opmærksom på følgende:

- Det skal understreges, at brugernavn og kode er personligt, og derfor ikke må deles med andre. Udleveres koden i forbindelse med for eksempel it-support, skal den efterfølgende ændres
- Forlader man pc´en, skal man huske at låse den (tryk **Ctrl**, **Alt**, **Del** og **Enter** for at låse), så uvedkommende ikke kan få adgang til Greve Kommunes data. Det samme gør sig gældende ved hjemmearbejde
- Man skal være opmærksom på hvem der har adgang/udsyn til skærmen, når der behandles personfølsomme data, ligesom man også skal være opmærksom på, at udskrifter med personfølsomme data ikke må ligge offentligt tilgængeligt
- Pc´en er et arbejdsredskab, og skal derfor primært bruges til fagligt relevante ting
- Når man er logget på Greve Kommunes netværk, skal man være opmærksom på hvad man foretager sig, da man repræsenterer Greve Kommune og dennes værdier
- Opstår der tvivl om, hvornår en handling er tilladt eller udgør en sikkerhedsrisiko, skal der rettes henvendelse til Center for Byråd & Økonomi for vejledning
- Husk altid at slukke pc og skærm, inden arbejdspladsen forlades.

Endelig forventes det, at den enkelte medarbejder reagerer aktivt på eventuelle it-sikkerhedsmæssige problemer eller fejl, og at medarbejderen i givet fald videregiver sine observationer til Center for Byråd & Økonomi.

Fratrædelse

Ved fratrædelse skal brugerinstruktøren eller it-vejlederen i det enkelte center informere Center for Byråd & Økonomi så det sikres, at den tidligere medarbejders adgange til Greve Kommune it-ressourcer fjernes helt. Ydermere skal centeret sørge for at få tilbageleveret alle de it-ressourcer den pågældende medarbejder har haft til rådighed under ansættelsen og sørge for at afslutte eventuelle teleabonnementer, datalinjer m.m., som måtte have været tilknyttet medarbejderen.

4. Logisk adgangsstyring

Generelt

Den logiske adgang til Greve Kommunes data og it-ressourcer kan kun ske via Greve Kommunes administrative it-netværk. Dette netværk er adskilt fra de øvrige netværk, der anvendes i kommunen, herunder den offentligt tilgængelige del af skolenetværket, biblioteksnetværket og andre eksterne net, som f.eks. Internettet.

Logisk adgangsstyring i Greve Kommune er organiseret således, at ansvaret for adgangstildeling er placeret hos brugerinstruktørerne i de enkelte centre. Center for Byråd & Økonomi er udførende og koordinerende faktor i forbindelse med adgangsstyring, ansvarlig for daglige retningslinjer og vejledning i brug af de logiske it ressourcer.

Målet med logisk adgangsstyring er at mindske risikoen for tab af fortrolighed, pålidelighed, integritet og tilgængelighed i Greve Kommune.

Brugeradministration

Standard brugeradministration

Supportfunktionen i Center for Byråd & Økonomi sørger for oprettelser, ændringer og sletninger af brugerprofiler på it-netværket på foranledning af brugerinstruktørerne i de enkelte centre og it-vejlederne på skolerne. I forbindelse med ansættelse, ændring eller sletning af en medarbejder sender en brugerinstruktør et brugerskema til Center for Byråd & Økonomi, der forestår den konkrete brugeradministration. Brugerskemaet findes på Mit Greve, udfyldes online, vedhæftes en sag i ServiceDesk og sendes til Supporten i Center for Byråd & Økonomi. På baggrund heraf sørger Center for Byråd & Økonomi for det ønskede adgangsniveau.

Center for Byråd & Økonomi sørger i forbindelse med fratrædelser for, at den fratrådte persons netværksdrev kan gøres tilgængelig i op til 6 måneder efter fratrædelsen. Herefter slettes netværksdrevet. E-postbokse slettes umiddelbart. I tilfælde af at man skal have adgang til en tidligere medarbejders e-postboks, kan dette ske i op til 180 dage efter sletning af brugerprofilen. Dette må dog kun finde sted efter, at der er indhentet en autorisation fra den relevante centerchef eller ansvarshavende direktør. Det samme gør sig gældende i forbindelse med en fratrådt medarbejders netværksdrev. I begge tilfælde skal det undlades at mapper benævnt *private* undersøges uden samtykke fra medarbejderen medmindre der er tale om tilfælde med mistanke om kriminelle forhold.

Administrator brugere

Udvalgte medarbejdere samt brugere fra Center for Byråd & Økonomi er autoriseret til at have administratorrettigheder. Disse personer er dokumenteret og autoriseret af it-chefen.
Udvalgte personer hos Greve Kommunes outsourcing partner på det it-driftsmæssige område vil også være autoriseret til at have administrator rettigheder. De personer og deres funktionsbeskrivelser vil ligeledes være dokumenteret af den person, som opretter brugerprofilerne.

Brugeradministration for fagsystemer

Adgang til fagsystemerne kræver særskilt autorisation på foranledning af en brugerinstruktør og godkendt af nærmeste leder, og oprettelserne foretages i de centre, der har systemejerskabet. Den enkelte medarbejder har selv ansvaret for installation af fagsystemet via det elektroniske softwarekatalog.

Fællesbrugerprofiler

Fællesbrugerprofiler er en brugerprofil på it-netværket, som kan oprettes i funktioner hvor flere medarbejdere har behov for at tilgå en pc-arbejdsplads uden rettigheder til andet end at logge på. Det vil typisk foregå i tilfælde, hvor flere medarbejdere tilgår det samme fagsystem på pc-arbejdspladsen, men først har behov at blive identificeret, når de tilgår fagsystemet.
Fællesbrugerprofiler skal altid vurderes og autoriseres af Center for Byråd & Økonomi, for at sikre at it-sikkerheden ikke kompromitteres.

Mit Greve bruger

Alle medarbejdere kan komme på Mit Greve med eget login via adressen https://mitgreve.greve.dk. Medarbejdere, der ikke er oprettet på Greve kommunes it-netværk, har også mulighed for at tilgå Mit Greve. Dette gøres ved, at den enkelte medarbejder opretter sig som bruger på adressen https://ssl.mit.greve.dk, og når medarbejderens brugerinstruktør har godkendt oprettelsen, er der adgang til Mit Greve. Medarbejderen har herefter læse-rettigheder til stort set alt på Mit Greve, og kan dermed se, hente og printe alle dokumenter og vejledninger, som alle andre medarbejdere på Greve Kommunes it-netværk.

Undtagelser for ovenstående er:

1. Medarbejderen har ikke adgang til "Mit websted" eller andre medarbejderes personlige websteder
2. Medarbejderen har ikke adgang til de websteder, projektrum, dokumentbiblioteker, mapper og filer, hvor de ansvarlige webredaktører har sat specifikke rettigheder (f.eks. "Skjulte dokumenter"-bibliotekerne på alle center websteder).

Kontroller

Periodiske kontroller sikrer, at medarbejdere ikke har adgang til flere it-ressourcer end deres funktion i Greve Kommune kræver. Ansvaret er placeret hos brugerinstruktørerne, som sørger for, at rettigheder bliver gennemgået minimum 1. gang årligt samt tildelt og fjernet ved ændringer i medarbejderes funktioner.

5. Styring af it-aktiver

Generelt

Center for Byråd & Økonomi står for den løbende vedligeholdelse og udskiftning af it-aktiver i Greve Kommune. Udskiftning sker kun i forbindelse med enheder, som ifølge Center for Byråd & Økonomis planlægning står til udskiftning.

Al it-anskaffelse finansieret af Greve Kommune skal ske gennem Supporten i Center for Byråd & Økonomi i en sag til Support. Privat udstyr kan anvendes på nogle at Greve Kommunes systemer jf. afsnittet **Anvendelse af mobilt udstyr** under kapitel 7.

Logiske it-aktiver (alle data som behandles på Greve Kommunes it-netværk) styres i forhold til retningslinjerne i persondataloven og sikkerhedsbekendtgørelsen, og det er det enkelte centers ansvar at klassificere de data, der behandles i centeret og sikre, at de er forsvarligt beskyttet. Center for Byråd & Økonomi bistår efter behov i klassificeringen.

Klassifikation af data og andre it-aktiver

Klassifikationen af data stiller forskellige krav til håndteringen og opbevaringen af data. Systemejeren skal ved introduktion af et nyt system og tilhørende hardware sikre, at sikkerheden i systemet er i stand til at beskytte de data, som systemet anvender i overensstemmelse med datas sikkerhedsklassifikation.

Dataklassificeringsniveauer

Dataklassifikationen er opdelt i følgende kategorier:

- Offentlige data – data, som kan offentliggøres til befolkningen på f.eks. kommunens hjemmeside, og som den enkelte borger uden videre kan begære indsigt i

- Ikke offentligt tilgængelige data – data, som er af en sådan beskaffenhed, at den enkelte borger ikke kan få indsigt i disse data. Eksempler på sådanne data er informationer om opbygningen af sikkerhed i kommunens administration, kontrakter, interne notater mv. Disse oplysninger kan være fortrolige efter andre regler end persondataloven
- Fortrolige oplysninger, der er omfattet af persondatalovens § 6 - Oplysninger som kun må behandles hvis:
    - personen (den registrerede) som oplysningerne omhandler, har givet sit samtykke hertil
    - det gøres for at overholde en retslig forpligtelse eller for at beskytte den registreredes interesser
    - det gøres af hensyn til udførelsen af en opgave i samfundets interesse, eller af hensyn til udførelsen af en opgave, der henhører under offentlig myndighedsudøvelse, som den dataansvarlige eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt
    - behandlingen er nødvendig for, at den dataansvarlige eller den tredjemand, til hvem oplysningerne videregives, kan forfølge en berettiget interesse og hensynet til den registrerede ikke overstiger denne interesse.

    Fortrolige oplysninger efter § 6 omfatter bl.a.:
    - Almindelige adresseoplysninger
    - Adressebeskyttelse
    - Identifikationsoplysninger
    - Økonomiske forhold

- Følsomme oplysninger, oplysninger omfattet af persondatalovens § 7 og 8- Oplysninger som kun må behandles hvis:
    - Personen (den registrerede) som oplysningerne omhandler, har givet samtykke hertil
    - Behandlingen er nødvendig for at beskytte den registreredes interesser
    - Behandlingen vedrører oplysninger som er offentliggjort af den registrerede eller er nødvendig for, at et retskrav kan fastlægges m.v.
    - Behandlingen er nødvendig for varetagelse af myndigheden opgaver

    Følsomme oplysninger, oplysninger omfattet af persondatalovens § 7 og 8
    - §7 – Oplysninger der omhandler racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold
    - §8 – Oplysninger der omhandler strafbare forhold, væsentlige sociale problemer og andre rent private forhold end de i § 7, stk. 1, nævnte, medmindre det er nødvendigt for varetagelsen af myndighedens opgaver.

Sikkerhedskrav til registreringen af følsomme og fortrolige data

Følgende er en oversigt over sikkerhedskrav til registreringen af data som indeholder fortrolige og følsomme oplysninger:

Autorisation	Systemejer skal autorisere brugeres adgang til data samt deres rettigheder til at læse, opdatere og slette data.
Adgangsforhold	Systemet skal adgangsbegrænses med bruger-ID og password.
Datakommunikation	Kommunikation af fortrolige og følsomme oplysninger over offentlige net skal krypteres ved "Send sikkert"-funktionen i Outlook.
Logning af adgang	Mislykkede adgangsforsøg logges og registreringerne herom gennemgås periodisk. Gentagne mislykkede forsøg skal medføre lukning af adgang.
Logning af anvendelse	Alle anvendelser af data vedrørende enkeltpersoner logges og gemmes i ½ og ved særlige behov op til 5 år (gælder ikke dokumenter under udarbejdelse). Loggen skal indeholde tidspunkt, bruger, anvendelse og personen, som anvendelsen vedrører.
Opbevaring	Dataene skal opbevares således at kun autoriserede brugere har adgang til dem. Alle data skal være omfattet af backup. Fysiske papirer skal opbevares i aflåste og brandsikre skabe.
Anmeldelse	Behandling af personoplysninger skal anmeldes til Datatilsynet.
Sletning	Data skal efter arkivering slettes fra de datamedier, de tidligere har ligget på. Er der tale om en kassation af de tidligere datamedier, skal datamedierne afleveres hos It, som sørger for en standardiseret og sikker sletning af indholdet.

Registrering af it-aktiver

Center for Byråd & Økonomi registrerer standard pc-arbejdspladser så det sikres, at de udskiftes med en fastlagt frekvens og dermed undgår at blive forældet.

Centrene og eksterne institutioner har selv ansvaret for at registrere og tyverisikre andre enheder såsom f.eks. mobiltelefoner, tablets osv. Det er vigtigt at alle enheders unikke IMEI nummer eller lignende er registreret i tilfælde af tyveri eller tab af enheder, da det skal bruges i forbindelse med forsikringskrav.

Dataene, der registreres for hvert it-aktiv, skal indeholde relationer og informationer således, at det er muligt af genetablere fra en katastrofe f.eks. lokation, ejer, backup, licenser, garanti, klassificering og service level agreements.

Tyverisikring
Alle pc-arbejdspladser skal markeres med tyverisikring.

Licenser
Center for Byråd & Økonomi har ansvaret for, at registrere standard licenser på alle standard installerede pc-arbejdspladser. Programmer som afviger fra standard installationer, og som kræver licens, skal afholdes og registreres af centrene selv.

Vedligeholdelse af it-aktiver

Alle fysiske it-aktiver er underlagt løbende vedligeholdelse i form af softwareopdateringer og eventuelle fysiske reparationer for at sikre driftsikkerheden på it-netværket og integriteten i dataene.

Kassation af it-aktiver

Kassation foretages af 3. part som ved certifikat verificerer, at it-aktiver, som Greve Kommune har afstået, kasseres i henhold til de krav, som dataenes klassifikation på disse aktiver kræver. Dvs. at det ikke er muligt at genskabe Greve Kommunes data efter afståelse.

6. Risikovurdering og håndtering

Generelt

Risikovurdering og -håndtering sikrer, at alle it-systemer og it-arbejdsgange i Greve Kommune risikovurderes og håndteres, således at it-brug altid foregår på den mest sikre og hensigtsmæssige måde og med forretningen Greve Kommune i fokus.
Center for Byråd & Økonomi kan bistå centrene i at risikovurdere de it-processer/-arbejdsgange, der finder sted, og hjælpe med at sikre, at identificerede risici dækkes af de rette kontroller.

Risikovurdering

Center for Byråd & Økonomi identificerer, vurderer og dokumenterer risici på baggrund af inputs fra organisationen, andre eksterne faktorer såsom lovkrav m.m. og har ansvar for en årlig it-revision.

Risikohåndtering

Center for Byråd & Økonomi håndterer risici på en måde, der sikrer, at årsagen til risiciene blotlægges, fjernes eller som minimum mindskes til et acceptabelt niveau. Udarbejdelse af kontroller og analyser af risiciene med henblik på løbende forbedring af it-sikkerheden sikrer proaktivt, at det acceptable niveau opnås, dvs. der hvor sikkerhedsforanstaltningerne står mål med risikoen.

7. Fysisk sikkerhed

Generelt

Fysisk sikkerhed fokuserer på sikkerheden omkring de fysiske it-zoner og beskyttelse af it-aktiver i Greve Kommune. Dette område varetages af risikokoordinatoren i Center for Teknik & Miljø i samarbejde med Center for Byråd & Økonomi.

Zoner

Zone 1 (omfatter serverrummet på rådhuset)

Den fysiske adgang til it-ressourcer i zone 1 er sikret med et elektronisk låsesystem, således at kun autoriserede personer kan få adgang til zonen. Adgang til zonen uden behørig autorisation må kun ske sammen med ledsager med en sådan autorisation. Grundlæggende må kun specifikke medarbejdere, afdelingslederen for intern service og rådhusbetjente have adgang til denne zone. Navngivne teknikere og håndværkere der har et godkendt behov, kan inden for normal arbejdstid eller i forbindelse med krisesituationer få uledsaget fysisk adgang til serverrummet. Øvrige personer må kun få adgang med autoriseret ledsager.

Lister over udstedte nøglekort gennemgås årligt med henblik på at revurdere, hvilke medarbejdere, navngivne teknikere og håndværkere, der har adgang til zonen.

Serverrummets gulv er hævet en halv meter i forhold til kælderetagens normale gulvhøjde for at modstå eventuelle svære oversvømmelser. Serverrummet indeholder ligeledes køling og ekstra brandslukning/ -alarmeringsudstyr samt UPS i tilfælde af strømafbrydelser. Serverrummets overvågnings- og beskyttelsesudstyr gennemses og testes årligt af autoriserede teknikere.

Alarmer viderestilles til Center for Byråd & Økonomis medarbejdere, rådhusbetjentene eller Falck afhængig af den aktuelle alarm.

Zone 2 (omfatter it-lager og it-værksted)

Den fysiske adgang til denne zone er sikret med et elektronisk låsesystem, således at kun autoriserede personer har adgang til zonen. Grundlæggende er det kun medarbejdere fra Center for Byråd & Økonomi, afdelingslederen for intern service og rådhusbetjente, der har adgang til denne zone. Teknikere og håndværkere fra firmaer, der har et godkendt behov, kan inden for normal arbejdstid eller i forbindelse med krisesituationer få uledsaget fysisk adgang til it-lager og -værksted.

Lokaler under zone 2 er endvidere sikret og overvåges i relation til uautoriseret indtrængen.

Lister over udstedte nøgler, nøglekort, adgangskoder mv. til zone 2 gennemgås årligt af Risikokoordinatoren og Center for Byråd & Økonomi med henblik på at revurdere, hvilke medarbejdere i Greve Kommune, der har adgang til zonen.

Zone 3 (Kontorer i Center for Byråd & Økonomi, krydsfelter, serverrum på eksterne lokationer mv.)
Den fysiske adgang til denne zone er sikret med specifikke låse, som kun autoriserede personer har nøgler til. På rådhuset vil det være medarbejdere fra Center for Byråd & Økonomi, afdelingslederen for intern service, rådhusbetjentene og navngivne teknikere og håndværkere fra firmaer med et godkendt behov, der har adgang til denne zone. På andre lokaliteter vil adgangen være baseret på autorisation fra den lokale leder i samråd med Center for Byråd & Økonomi.

8. Brug af it-udstyr

Generelt

Brug af it-udstyr fokuserer på den bruger- og filsikkerhed, som er forbundet med brugen af it-udstyr på Greve Kommunes it-netværk hvad enten der er tale om mobilt, privat eller it-udstyr leveret af Greve Kommune.

Filbehandling

Al filbehandling med undtagelse af følsomme data, skal foregå på Mit Greve. Alle medarbejdere er tildelt et personligt websted på Mit Greve.
Greve Kommune forbeholder sig ret til, med samtykke fra centerchef eller direktør at foretage gennemgang af alle systemer og personlige/private områder f.eks. på Mit Greve, netværksdrev, mobiltelefoner, i e-post og andre områder og enheder som måtte indeholde data fra Greve Kommune, såfremt der forefindes berettigede interesser for dette jf. afsnittet *Standard brugeradministration*. Disse interesser er af hensyn til Greve Kommunes drift, sikkerhed, genetablering og dokumentation samt hensynet til kontrol af medarbejderes brug. Alle gennemgange foretages under fuld fortrolighed og med den enkelte medarbejders vidende, medmindre det skønnes at medarbejderens vidende kan kompromittere evt. bevismateriale f.eks. i forbindelse med gennemgange foretaget med baggrund i en mistanke om kriminelle forhold.

Elektronisk udveksling af data
Det er ikke tilladt at anvende uautoriserede og usikre datamedier – f.eks. Dropbox, usb-nøgler m.m. - til udveksling af data eller arkivering af data, som indeholder fortrolige eller følsomme oplysninger.

Data med fortrolige og følsomme oplysninger

Kommunikation af data med fortrolige eller følsomme oplysninger over offentlige netværk mellem Greve Kommune og driftsleverandører, hjemmearbejdspladser mv. skal krypteres i henhold til data-klassifikationen. Som bruger skal man derfor altid sende data via "Send sikkert"-funktionen i Outlook, hvis dataene skal sendes udenfor Greve Kommunes it-netværk.

Adgangskode politik

Brug af adgangskoder

Alle nye medarbejdere skal ændre adgangskode ved første logon, og adgangskodepolitikken i Greve Kommune kræver, at en adgangskode:

- Minimum består af 8 karakterer
- Består af 3 af følgende 4 tegnmuligheder: store bogstaver, små bogstaver, tal og specialtegn
- Ikke indeholder dit navn eller brugernavn
- Bliver ændret hver 3. måned
- Ikke ligner en af de 5 sidst benyttede adgangskoder
- Ikke kan slås op i en ordbog.

Husk at hvis du benytter en telefon, tablet computer eller lignende til at synkronisere din mail, skal du også ændre password på disse enheder, så snart du har ændret det på pc´en.

Dit ansvar som bruger

Som bruger på Greve Kommunes it-netværk skal du være opmærksom på følgende:

- Din adgangskode er personlig og må derfor ikke deles med andre eller skrives ned således, at den risikerer at blive offentliggjort
- Du skal skifte din adgangskode, hvis du er det mindste i tvivl, om den er blevet kompromitteret
- Din adgangskode bliver spærret, hvis du taster den forkert 5 gange. Support kan låse op, så du kan forsøge den samme adgangskode igen, men har du glemt din adgangskode og skal have den nulstillet, skal du henvende dig til din brugerinstruktør, som kan nulstille adgangskoden eller oprette en sag til Support via ServiceDesk.

Anvendelse af mobilt udstyr

Mobilt udstyr i Greve Kommune omfatter bærbare pc´ere, mobiltelefoner, tablet computere og lignende.

Benyttes bærbar pc på Greves it-netværk, skal den være installeret med standard Greve Kommune opsætning. Ydermere er det muligt at få adgang til Greves it-netværk via Citrix.

Mobiltelefoner, tablet computere og lignende må som udgangspunkt kun tilgå it-netværket via app´en DME fra Excitor, Citrix og Webmail. Det er kun tilladt at benytte Exchange ActiveSync på mobile enheder, hvis man ikke behandler følsomme eller fortrolige oplysninger jf. kapitel 5 i afsnittet "Dataklassificeringsniveauer".

Brug af privat it-udstyr

I Greve Kommune er det tilladt at benytte eget it udstyr på trådløst netværk. Det er kun tilladt at tilgå Greve Kommunes data på disse enheder via førnævnte DME, Citrix og Webmail løsninger.

Logning af adgang til Greve Kommunes it-ressourcer

Greve Kommune logger og registrerer alle mislykkede adgangsforsøg, anvendelser af data som indeholder fortrolige eller følsomme data samt medarbejdernes brug af hjemmesider via internettet og e-post. Greve Kommune forbeholder sig ret til med centerchef eller direktørs samtykke, ved begrundet mistanke til enhver tid at gennemgå disse registreringer under samme forudsætninger som beskrevet i afsnittene *Standard brugeradministration* og *Filbehandling* omkring adgang til medarbejderes e-postkasser og personlige netværksdrev.

9. Driftsafviklingsprocedurer

Generelt

Center for Byråd & Økonomi har outsourcet driftsansvaret for Greve Kommunes serverpark til en ekstern leverandør. Center for Byråd & Økonomi samarbejder løbende med leverandøren om, at driftsafviklingen foretages på en stabil, kvalificeret og sikker måde således, at fortroligheden, pålideligheden, integriteten og tilgængeligheden af it-ressourcerne og deres data sikres. Det indebærer kontroller af de medarbejdere, som leverandøren benytter på Greve Kommunes ressourcer. Ligesom det indebærer, at it-ressourcerne som udgangspunkt er tilgængelige for medarbejderne, borgerne og virksomhederne døgnet rundt, dog vil eventuelle driftsnedbrud primært blive udbedret inden for normal arbejdstid. Længerevarende nedlukninger af it-ressourcer skal så vidt muligt ske uden for normal arbejdstid. Ved kritiske systemnedbrud træder it-beredskabsplanen i kraft.

Backup og genetablering

For, til enhver tid, at kunne fremfinde informationer i forbindelse med kommunens aktiviteter, har Center for Byråd & Økonomi ansvaret for, at der tages daglig backup via ekstern leverandør.
Backup foretages i overensstemmelse med dataklassifikation, forretnings- /lovgivningskrav og it-beredskabsplanlægningen i kommunen.

For at sikre, at data kan genindlæses ved nedbrud, foretager Center for Byråd & Økonomi verifikation af sikkerhedskopier ved hjælp af løbende genetableringstests.

Hele Greve Kommunes data backup opbevares sikkert og udenfor kommunens lokaliteter således, at disse altid kan fremfindes ved igangsættelse af nødplaner eller i forbindelse med andet behov.

For at backupfunktionen ikke kompromitterer sikkerheden af de data, der tages backup af, er der opsat adgangskontrol således, at uautoriserede personer ikke kan få adgang til oplysninger via arkiverede filer. Backup er outsourcet til 3. part, og filer krypteres ved transmittering over offentlige net.
Center for Byråd & Økonomi er autoriseret til at reetablere filer. Reetablering foregår således, at det, ved genindlæsning af filer, sikres, at der ikke ændres på ejer og adgangsrettigheder.
I forbindelse med backup og reetablering udarbejdes en log, der dokumenterer, hvilke filer der er blevet arkiveret og reetableret. Loggen gennemgås og gemmes som dokumentation for arkiveringen og reetableringen.

Logning i forbindelse med it-ressourcer

Center for Byråd & Økonomi sikrer, at der foretages overvågning af netværkskomponenter og andet it-udstyr, herunder den fysiske sikring af zone 1 - serverrummet. Dette bliver foretaget via en automatisk overvågning, hvor det sikres, at der følges op på eventuelle fejl, problemer eller sikkerhedsmæssige hændelser, der måtte kræve nærmere undersøgelse eller opfølgning. Hændelserne registreres automatisk i Support i Center for Byråd & Økonomi.

Al overvågning af servere foretages af den eksterne leverandør i henhold til indgåede kontrakt om outsourcing.

Alle ure i it-netværket er synkroniseret med en præcis tidsangivelseskilde for at sikre tidsangivelser i loggen stemmer overens på tværs af systemer.

10. Netværket

Generelt

Greve Kommunes it-netværk er segmenteret med henblik på at sikre de transmitterede data og den underliggende infrastruktur. Center for Byråd & Økonomi står for driften af netværket.

Segmentering

Kommunikationsadskillelsen mellem netværk sker med udgangspunkt i, at intet er tilladt, medmindre der specifikt foreligger en begrundet godkendelse af den specifikke kommunikationssammenkobling. Center for Byråd & Økonomi har det sikkerhedsmæssige ansvar herfor, og It-chefen foretager godkendelse

heraf. I tvivlstilfælde er det It-sikkerhedsudvalget, som tager stilling til de sikkerhedsmæssige aspekter i netværksopsætningen.

Netværksudstyr på hjemmearbejdspladser og eksterne institutioner

Autoriserede eksterne tilslutningsforbindelser er ADSL-forbindelser fra hjemmearbejdspladser og eksterne institutioner, samt Citrix-opkoblinger fra mobility- og private pc´ere på standard ADSL-forbindelser.

Trådløse netværk

Der er tre typer trådløse netværk i Greve Kommunes it-netværk. Det første bruges til det administrative net og kræver, at den enkelte pc som prøver at tilgå det, er godkendt og har fået tildelt certifikat. Det samme gør sig gældende for det andet netværk, som bruges på kommunens skoler. Dette netværk er adskilt fra det administrative net.

Det tredje netværk er adskilt fra de to ovenstående netværk og bruges som internetforbindelse til gæster og lignende på Greve Rådhus. Ved tilgang til dette netværk, skal man som bruger acceptere Greve Kommunes retningslinjer for brug herpå.

11. Support

Generelt

Alle sager til It skal gå igennem Support, som vurderer og håndterer sagerne efter ITIL principperne.

Supports brug af ITIL-processerne sikrer:

- at it-problemer altid bliver vurderet ud fra væsentligheden, således at problem og eventuelle dybere liggende årsager samt eventuelle sikkerhedsbrister korrigeres
- at medarbejdere deltager aktivt i rettelse af fejl, løsning af problemer og forbedring af it-sikkerheden
- at den netværksansvarlige foranlediger, at der føres log over alvorlige hændelser med henblik på at opretholde dokumentation af hændelsesforløb
- at sager eskaleres til teknisk support hos den eksterne leverandør om nødvendigt.

Standard ændringer

Center for Byråd & Økonomi har i forbindelse med udviklingen af ITIL Change management-processen defineret et omfang for standard ændringer, som kan godkendes og implementeres uden testforløb og risikovurderinger. Standard ændringer er bl.a. tilføjelse af allerede godkendte pc´ere på it-netværket, automatisk opdatering af antivirus på pc-arbejdspladserne eller brugeradministration.

Alle konfigurationsændringer planlægges, kvalitetssikres og godkendes inden implementering. Derved sikres det, at ændringer i konfigurationen af hardware og software skaber færrest mulige negative konsekvenser for sikkerheden på it-netværket.

Implementeringer på netværk

I forbindelse med implementering af servere, pc'er, netværkskomponenter, printer eller andet it-udstyr på netværket vurderer Center for Byråd & Økonomi risiciene i forbindelse hermed igennem ITIL Change management-processen.

Ansvaret for ændringer i konfigurationen af netværk, servere, platforme, operativsystemer, database-systemer mv. påhviler Center for Byråd & Økonomi. Dette gælder alt fra centrale servere og netværks-udstyr til medarbejdernes pc'ere, smartphones og hjemme-pc'ere konfigureret med Greve Kommunes standard image.

Varsling

Center for Byråd & Økonomi skal sørge for, at alle berørte brugere varsles i god tid inden implementering af større eller væsentlige konfigurationsændringer, som kan påvirke brugernes anvendelse af it. Samtidig informeres brugerinstruktørerne om eventuelle konsekvenser ved ændringen.

12. Beskyttelse mod ondsindet programmel

Generelt

Ondsindet programmel udgør en stor trussel mod tilgængelighed af systemer samt fortrolighed og integritet af data. Center for Byråd & Økonomi har derfor etableret en veldefineret og effektiv beskyttelse mod ondsindede programmer.

Antivirus og antispam

Samtlige servere i Greve Kommune og pc-arbejdspladser med adgang til Greve Kommunes administrative netværk er beskyttet mod ondsindet programmel, som eksempelvis virus og orme. Herudover bliver al ind og udgående e-post skannet for ondsindet software før videresendelse til den interne eller den eksterne modtager.

På pc-arbejdspladserne er beskyttelsen etableret, således at potentielt kritiske filer scannes i forbindelse med åbningen på pc'en. Denne beskyttelse kan ikke deaktiveres eller afinstalleres af medarbejderne.

Opdateringen af beskyttelsesværktøjet i relation til virusmønstre mv. sker via central server. Servere og pc-arbejdspladser opdateres automatisk af den eksterne leverandør/outsourcingpartner, når det er påkrævet.

Beskyttelsesværktøjet er konfigureret således, at Center for Byråd & Økonomi informeres i tilfælde af, at der er identificeret en virus eller lignende på en af Greve Kommunes servere eller pc-arbejdspladser. Potentielle filer og e-post, der identificeres som indeholdende vira mv., isoleres, med henblik på en nærmere manuel verifikation, der kun foretages af medarbejdere fra Center for Byråd & Økonomi.

13. Anskaffelse og vedligeholdelse af fagsystemer

Generelt

Fagsystemerne indgår som et væsentligt element i det daglige arbejde i Greve Kommune. Det er derfor af vital betydning, at nyanskaffelser og opdateringer af disse lever fuldt op til den eksisterende kvalitets- og sikkerhedsstandard, herunder krav til systemdokumentation. Alle nye systemer bliver derfor og risikovurderet og håndteret derefter, inden eventuel implementering kommer på tale.

Greve Kommune har samtidig har valgt ikke at påtage sig udvikling af eget programmel i nævneværdigt omfang og anvender udelukkende pålidelige og kompetente leverandører.

Fagsystemer

Anskaffelse af fagsystem

Center for Byråd & Økonomi skal involveres i enhver anskaffelse af nye fagsystemer. Involveringen skal ske på et så tidligt tidspunkt, at Center for Byråd & Økonomis krav og råd kan inddrages i vurderingen og forhandlingen om det nye system.

Center for Byråd & Økonomi sørger ved indkøb af et nyt fagsystem for at foretage en teknisk gennemgang af installationen af fagsystemet for at sikre, at dette lever op til det ønskede sikkerhedsniveau i Kommunen, og at det ikke kompromitterer andre systemers sikkerhed. Dette omfatter en gennemgang af den tekniske platform og integration med øvrige systemer.

Når et nyt system indkøbes, bliver centerchefen i det enkelte center systemejer. Centerchefen kan delegere de konkrete opgaver til en medarbejder, der bliver systemansvarlig for systemet. Systemejerens ansvar er beskrevet i "Vejledning i systemejerskab i Greve Kommune".

Selve installationen af serversoftware og klienter foretages af leverandøren i samarbejde med Center for Byråd & Økonomi. Center for Byråd & Økonomi leverer den nødvendige platform bestående af pc-arbejdspladser, operativsystem og eventuelle databasesystemer, som leverandøren kan installere på.

Hvis et givet fagsystem kræver, at der foretages ændringer i standardkonfigurationen, gennemgås, godkendes og foretages dette af Center for Byråd & Økonomi igennem change processen.

Vedligeholdelse af fagsystemer

Systemejerne har ansvaret for opgradering/patching mv. af fagsystemerne (se afsnit 2 "Organisation og ansvar"). Alle ændringer til fagsystemerne foretages så vidt muligt af leverandøren. Dette skal af systemejerne varsles til Center for Byråd & Økonomi i god tid, og Center for Byråd & Økonomi vil bistå og overvåge implementeringen af ændringerne. Såfremt der er tale om væsentlige ændringer, som medfører ændringer i det eksisterende sikkerhedsniveau eller krav til dette, eller som påkræver ændringer i operativsystem, databasesystem mv., skal dette godkendes af Center for Byråd & Økonomi, som hvis der var tale om et nyt system.

Inden der gives logisk adgang til servere og systemer, skal Center for Byråd & Økonomi have godkendt den pågældende leverandør og sørget for, at der foreligger en underskrevet tro og love erklæring fra leverandøren. Derudover skal konsulenternes brugerprofiler disables, når de ikke bruges.

14. Samarbejdspartnere og leverandører

Generelt

Det er hensigten, at Center for Byråd & Økonomi indgår service level agreements (SLA) med alle interne såvel som eksterne samarbejdspartnere og leverandører med hjælp fra ITIL-processen Service Level Management således, at forventninger bliver afstemt, og samarbejdet derved understøtter Greve Kommune på den bedst mulige måde.

Før samarbejde

Før et samarbejde indgås og kontrakten underskrives, aftales it-leverancen så den er målbar og kan vurderes ud fra forventningerne afstemt i SLA´en. Således sikres det, at forventninger til samarbejdet er formaliseret inden start. Derudover sikrer Center for Byråd & Økonomi, at samarbejdet er sikkerhedsmæssigt forsvarligt ved hjælp af bl.a. tro og love erklæringer og i forhold til Greve Kommunes retningslinjer i indeværende politik.

Under samarbejde

Center for Byråd & Økonomi foretager sammen med samarbejdspartneren eller leverandøren løbende vurderinger af samarbejdet og indholdet i SLA´en, så forventninger løbende bliver afstemt.

Afslutning af samarbejde

Ved afslutning af samarbejdet sørger Center for Byråd & Økonomi for arkivering af relevant dokumentation samt nedlæggelse af brugerprofiler og forbindelser til Greve Kommunes it-netværk.

15. Beredskabsplanlægning

Generelt

Center for Byråd & Økonomi har udarbejdet en it-beredskabsplan, som indgår i det overordnede beredskab for hele Greve Kommune. Beredskabet sikrer, at Greve Kommune i tilfælde af større driftsnedbrud eller egentlige katastrofer er i stand til at genoptage kritiske aktiviteter i de enkelte centre og institutioner inden for en acceptabel tidshorisont. De større driftsnedbrud eller katastrofer betyder tab af tilgængelighed af væsentlige systemer, udstyr og/eller faciliteter, hvorfor reetablering af tilgængeligheden af disse er et centralt område i beredskabsplanlægningen.

Yderlige informationer såsom test, vedligeholdelse og organisering er beskrevet i it-beredskabsplanen.

16. TV-overvågning og brug af digitale billeder

Generelt

Tv-overvågning i Greve Kommune sker efter reglerne i "Bekendtgørelse af lov om tv-overvågning", og brugen af tv-overvågning i kommunen er anmeldt til Datatilsynet.

Brug af digitale billeder i kommunen er omfattet af persondataloven, og de ansatte vejledes i håndteringen af digitale billeder igennem "Vejledning i brug af billeder i Greve Kommune".

17. Brug af sociale medier

Generelt

Brugen af sociale medier er beskrevet i "Retningslinjer for brug af sociale medier i Greve Kommune".

Arbejdsmæssig brug af sociale medier

Ved arbejdsmæssig brug af sociale medier skal det sikres, at brugerkonti på medierne er forbundet til en fælles postkasse i det pågældende center. Når medarbejdere kommunikerer med borgerne via medierne,

skal det foregå via en personlig arbejdsmæssig profil, så det altid er tydeligt, hvem der har stået for kommunikationen. Denne profil må ikke benyttes til privat brug.

Privat brug af sociale medier

Som medarbejder i Greve Kommune er det vigtigt at overholde "Retningslinjer for brug af sociale medier i Greve Kommune", når sociale medier benyttes privat, så det sikres at der ikke bliver kommunikeret kompromitterende data på nettet.